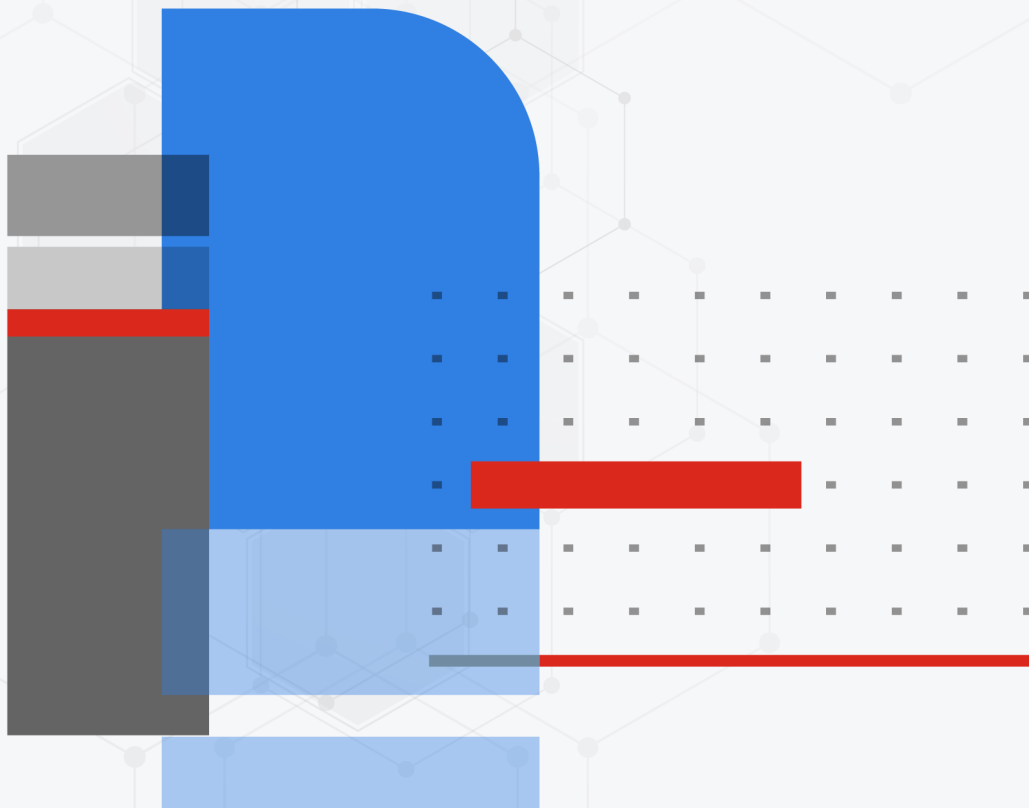




# New Features Guide

FortiAnalyzer 7.4.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



July 17, 2023

FortiAnalyzer 7.4.0 New Features Guide

05-740-898228-20230717

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Overview</b>	<b>6</b>
<b>Fabric View</b>	<b>7</b>
Connectors	7
Webhook Connector to Support MS Teams	7
<b>Security Operations (SOC)</b>	<b>9</b>
Asset and Identity	9
New charts in the Asset Identity Center	9
Others	10
FortiSoC GUI reorganization	11
Notifications for new Outbreak Alerts 7.4.1	14
<b>Log and Report</b>	<b>16</b>
Logging	16
FortiAnalyzer supports FortiWeb Cloud attack logs	16
Support parsing and addition of third-party application logs to the SIEM DB	17
Per-ADOM log rate	22
Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1	24
Logging support for FortiCASB 7.4.1	26
Logging support for FortiPAM 7.4.1	28
Logging support for FortiToken Cloud 7.4.1	29
Log Forwarding	30
Fluentd support for public cloud integration	30
Reports	34
Report guidance	34
PCI Security Rating Report	36
Cyber Threats Assessment Report update	37
Threat Report update	38
FSBP Security Rating Report	40
CIS Controls Security Rating report	41
Shadow IT Report	42
FortiADC Report 7.4.1	43
Default ZTNA Report 7.4.1	45
Others	46
Time zone settings per ADOMs/Reports	46
<b>System</b>	<b>50</b>
Others	50
FortiAnalyzer GUI enhancements	50
Fabric of FAZ topology chart	54
Fabric of FAZ: member authorization with supervisor	56
Fabric of FAZ global FortiView support	61
Fabric of FAZ: Central report support and creating Fabric groups	63
Block out contract device from upgrading to next or major or minor release	66

---

<b>Cloud Services</b>	<b>70</b>
FortiAnalyzer supports FortiCare Elite Service	70
<b>Operational Technology</b>	<b>74</b>
Operational Technology (OT) Security Service	74
OT Purdue Model in a consolidated Asset & Identity Center Dashboard	76
OT Security Risk Report	79
<b>Index</b>	<b>82</b>
7.4.0	82
Fabric View	82
Security Operations	82
Log and Report	82
System	83
Cloud Services	83
Operational Technology	83
7.4.1	83
Security Operations	83
Log and Report	83



# Change Log

Date	Change Description
2023-05-15	Initial release.
2023-05-16	Added: <ul style="list-style-type: none"><li>• <a href="#">Per-ADOM log rate on page 22</a></li><li>• <a href="#">Fabric of FAZ: Central report support and creating Fabric groups on page 63</a></li></ul>
2023-05-19	Added: <ul style="list-style-type: none"><li>• <a href="#">Webhook Connector to Support MS Teams on page 7</a></li><li>• <a href="#">Report guidance on page 34</a></li><li>• <a href="#">CIS Controls Security Rating report on page 41</a></li></ul>
2023-05-31	Added <a href="#">Operational Technology on page 74</a> .
2023-06-16	Added: <ul style="list-style-type: none"><li>• <a href="#">FortiSoC GUI reorganization on page 11</a></li><li>• <a href="#">New charts in the Asset Identity Center on page 9</a></li><li>• <a href="#">Shadow IT Report on page 42</a></li><li>• <a href="#">Time zone settings per ADOMs/Reports on page 46</a></li></ul>
2023-06-21	Added <a href="#">Fluentd support for public cloud integration on page 30</a> .
2023-06-30	Added <a href="#">Operational Technology (OT) Security Service on page 74</a> .
2023-07-17	Updated <a href="#">Time zone settings per ADOMs/Reports on page 46</a> .
2023-08-31	Initial release of FortiAnalyzer 7.4.1.

# Overview

This guide provides details of new features introduced in FortiAnalyzer 7.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiAnalyzer new features are organized into the following categories:

- [Fabric View on page 7](#)
- [Security Operations \(SOC\) on page 9](#)
- [Log and Report on page 16](#)
- [System on page 50](#)
- [Cloud Services on page 70](#)
- [Operational Technology on page 74](#)

For a list of all features organized by the version number that they were introduced, see [Index on page 82](#).

# Fabric View

This section lists the new features added to FortiAnalyzer for Fabric View:

- [Connectors on page 7](#)

## Connectors

This section lists the new features added to FortiAnalyzer for connectors:

- [Webhook Connector to Support MS Teams on page 7](#)

## Webhook Connector to Support MS Teams



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

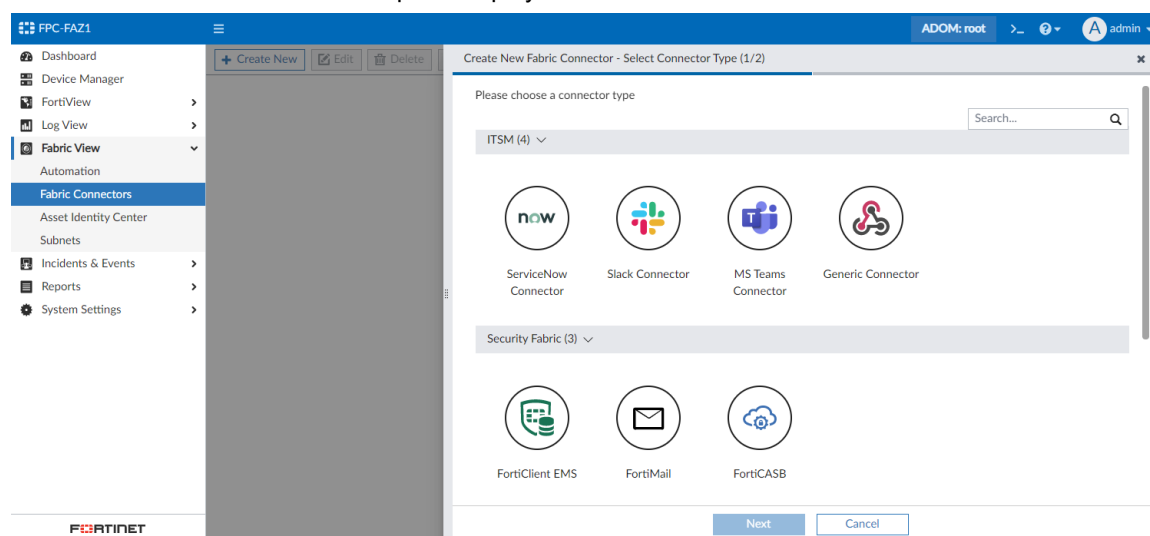
- [Creating or editing ITSM connectors](#)

A webhook connector has been added in FortiAnalyzer to support MS Teams. This connector can be used to post a message in MS Teams.

### To create a MS Teams connector:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*.

The *Create New Fabric Connector* pane displays.



3. In the *ITSM* section, double-click *MS Teams Connector*.

## 4. Configure the following options:

<b>Name</b>	Type a name for the fabric connector.
<b>Description</b>	(Optional) Type a description for the fabric connector.
<b>Protocol</b>	Select HTTPS.
<b>Method</b>	Select POST.
<b>Title</b>	Type a title for the fabric connector.
<b>Teams Webhook URL</b>	Enter the incoming webhook URL created in MS Teams.
<b>HTTP Body</b>	Enter the HTTP body of the message that should be sent by the connector. For example, { \"text\": \"<message to send>\" }.
<b>Status</b>	Enabled by default. The connector can be disabled, as needed.

The screenshot displays the 'Create New Fabric Connector - MS Teams Connector (2/2)' configuration window in the FortiAnalyzer interface. The window is titled 'Create New Fabric Connector - MS Teams Connector (2/2)' and has a close button (X) in the top right corner. The interface is divided into two main sections: 'Connector Settings' and 'Microsoft Teams'.

**Connector Settings:**

- Name:** Send message to MS Teams
- Description:** (Empty text area)
- Protocol:** HTTPS (Selected)
- Method:** POST (Selected)
- Title:** Alert
- Teams Webhook URL:** https://outlook.office.com/webhook/xxxxxx/IncomingWebhook/xxxxxx/xxxxxx
- HTTP Body:** ["text": "<message to send>"]
- Status:** Enabled (Toggle switch is turned on)

**Microsoft Teams:** (Empty section)

The interface includes a sidebar on the left with navigation options: Dashboard, Device Manager, FortiView, Log View, Fabric View, Automation, Fabric Connectors, Asset Identity Center, Subnets, Incidents & Events, Reports, and System Settings. The top bar shows the user is logged in as 'admin'.

## 5. Click OK.

# Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- [Asset and Identity on page 9](#)
- [Others on page 10](#)

## Asset and Identity

This section lists the new features added to FortiAnalyzer for asset and identity:

- [New charts in the Asset Identity Center on page 9](#)

### New charts in the Asset Identity Center

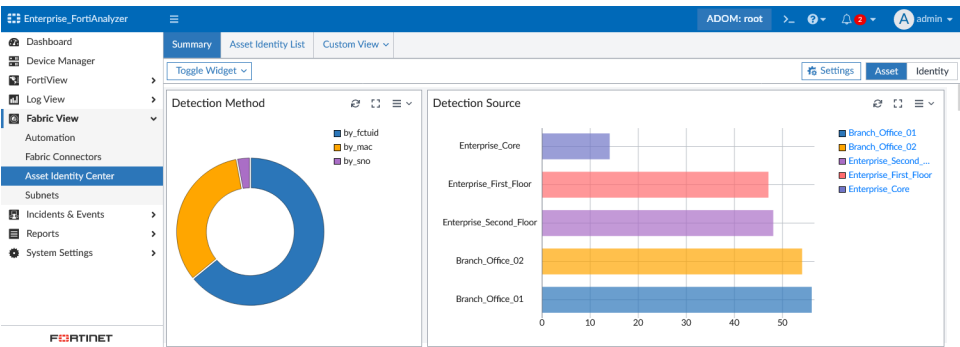


This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [Asset Summary](#)
- [Identity Summary](#)

The new *Asset Identity Center* pane combines the previous *Asset Center* and *Identity Center* panes. There are new and updated widgets in the *Asset Identity Center*, which can be used for analysis of endpoints and end users.

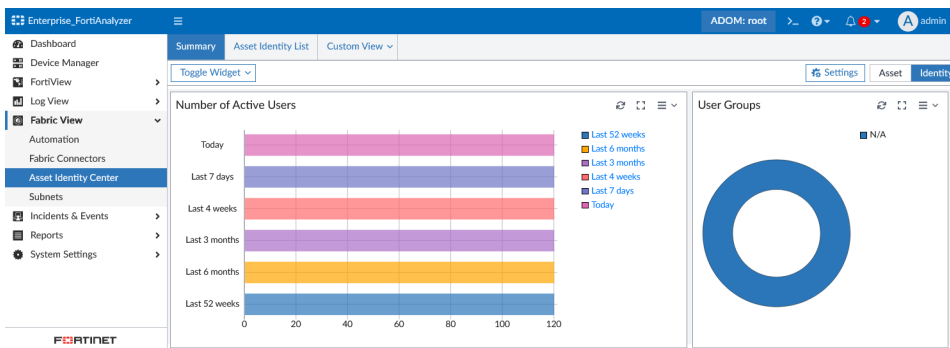
Go to *Fabric View > Asset Identity Center > Summary*. By default, the pane displays the *Asset* dashboard. You can click *Identity* to display the *Identity* dashboard. From the *Toggle Widgets* dropdown, select which widgets should display on the dashboard. You can filter all widgets on the dashboard from *Settings*.



The *Asset* dashboard includes the following widgets:

<b>Detection Method</b>	Displays endpoint detections by method.
<b>Detection Source</b>	Displays a breakdown of the asset center data sources.
<b>Identification/Unidentified Asset</b>	Displays the number of detected endpoint assets that are identified and unidentified.

<b>Hardware/OS Distribution</b>	Displays endpoint hardware operating system distribution.
<b>Discovery Timeline</b>	Displays an asset discovery timeline.
<b>Identified Active Asset</b>	Displays identified asset visibility over the past 24 hours to 52 weeks.
<b>Assets By Location</b>	Displays identified assets by location.
<b>Identified Activity Timeline</b>	Displays a first seen, last update, and last seen identified asset activity timeline.
<b>Changes Timeline</b>	Displays an asset changes timeline.
<b>Unidentified Active Asset</b>	Displays unidentified asset visibility over the past 24 hours to 52 weeks.
<b>Unidentified Activity Timeline</b>	Displays a first seen, last update, and last seen unidentified asset activity timeline.



The *Identity* dashboard includes the following widgets:

<b>Top Users</b>	Displays asset user data.
<b>Number of Active Users</b>	Displays user visibility data over the past 24 hours to 52 weeks.
<b>User Groups</b>	Displays user groups.
<b>User's Location</b>	Displays user numbers by location.
<b>User's Manager</b>	Displays user numbers by manager.
<b>Discovery Timeline</b>	Displays the user discovery timeline.
<b>Activity Timeline</b>	Displays the user activity timeline.
<b>Endpoint Tag Distribution</b>	Displays the distribution of endpoint tags.

## Others

This section lists the new features added to FortiAnalyzer for other topics related to security operations:

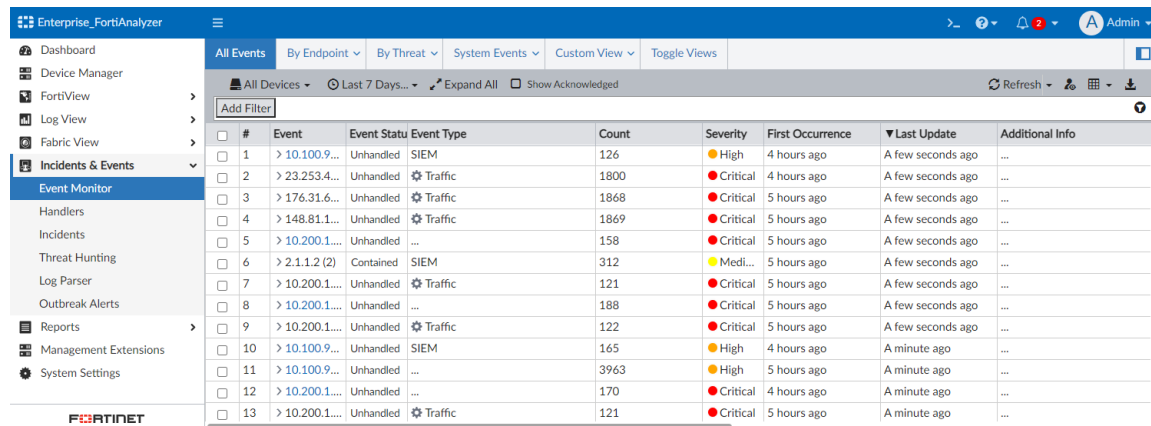
- [FortiSoC GUI reorganization on page 11](#)
- [Notifications for new Outbreak Alerts 7.4.1 on page 14](#)

## FortiSoC GUI reorganization

The *FortiSoC* features have been organized in the following areas of the GUI:

- *Incidents & Events*
- *FortiView*
- *Fabric View*

To create and manage events, go to *Incidents & Events*.

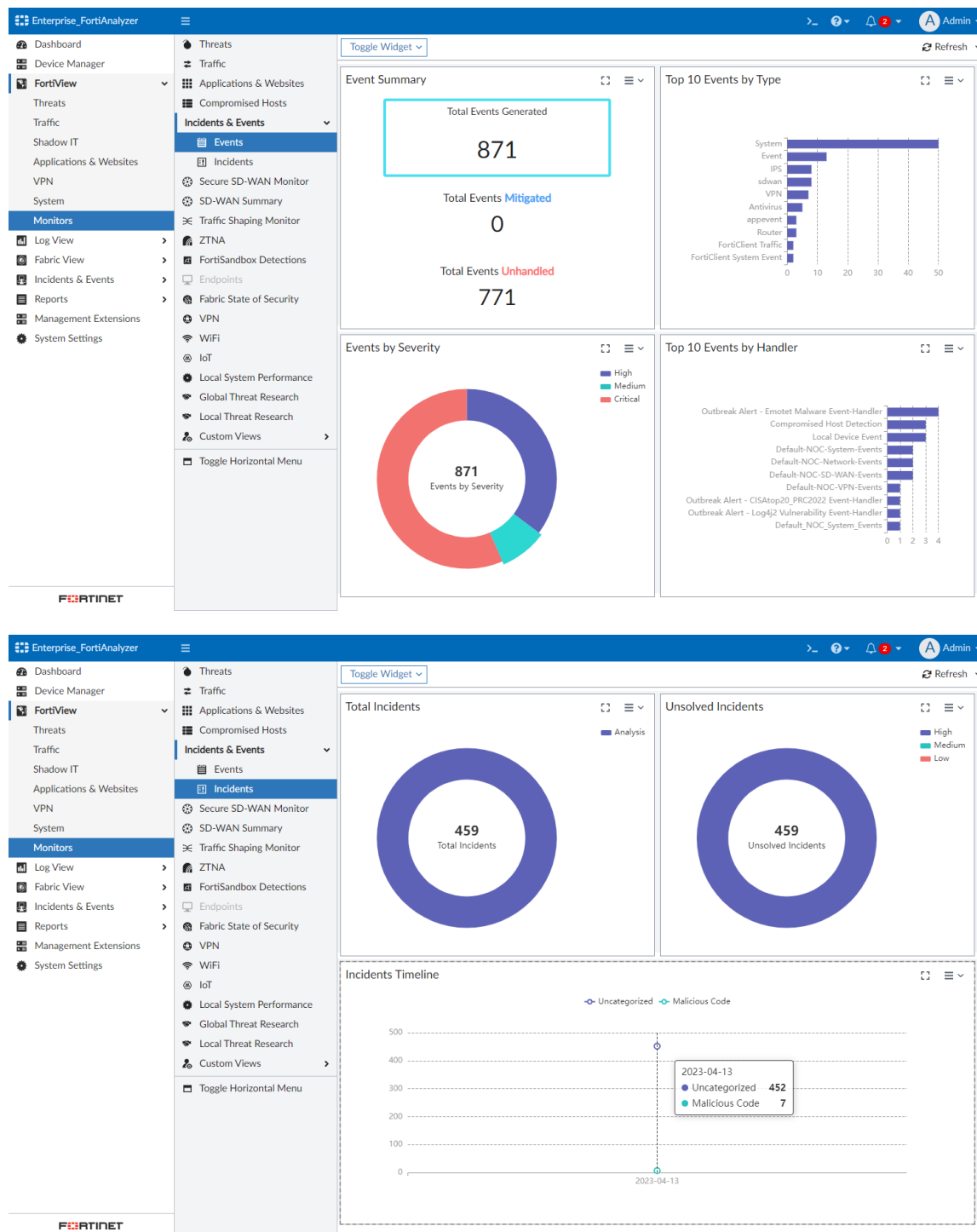


#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info
1	> 10.100.9...	Unhandled	SIEM	126	High	4 hours ago	A few seconds ago	...
2	> 23.253.4...	Unhandled	Traffic	1800	Critical	4 hours ago	A few seconds ago	...
3	> 176.31.6...	Unhandled	Traffic	1868	Critical	5 hours ago	A few seconds ago	...
4	> 148.81.1...	Unhandled	Traffic	1869	Critical	5 hours ago	A few seconds ago	...
5	> 10.200.1...	Unhandled	...	158	Critical	5 hours ago	A few seconds ago	...
6	> 2.1.1.2 (2)	Contained	SIEM	312	Medium	5 hours ago	A few seconds ago	...
7	> 10.200.1...	Unhandled	Traffic	121	Critical	5 hours ago	A few seconds ago	...
8	> 10.200.1...	Unhandled	...	188	Critical	5 hours ago	A few seconds ago	...
9	> 10.200.1...	Unhandled	Traffic	122	Critical	5 hours ago	A few seconds ago	...
10	> 10.100.9...	Unhandled	SIEM	165	High	4 hours ago	A minute ago	...
11	> 10.100.9...	Unhandled	...	3963	High	5 hours ago	A minute ago	...
12	> 10.200.1...	Unhandled	...	170	Critical	4 hours ago	A minute ago	...
13	> 10.200.1...	Unhandled	Traffic	121	Critical	5 hours ago	A minute ago	...

*Incidents & Events* includes the following:

<b>Event Monitor</b>	View events generated by event handlers. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Handlers</b>	Configure data selectors, notification profiles, basic event handlers, and correlation event handlers. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Incidents</b>	Create and update incidents to track and analyze events. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Threat Hunting</b>	View a log count chart and SIEM log analytics table. The <i>Threat Hunting</i> dashboard is only available in Fabric ADOMs when ADOMs are enabled. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Log Parser</b>	View and manage SIEM log parsers. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Outbreak Alerts</b>	View outbreak alerts and automatically download related event handlers and reports from FortiGuard. The FortiAnalyzer Outbreak Detection Service is a licensed feature. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .

To review incidents and events in dashboards, go to *FortiView > Monitors > Incidents & Events*.



FortiView > Monitors > Incidents & Events includes the following dashboards:

## Events

This dashboard includes the following widgets:

- *Event Summary*
- *Top 10 Events by Type*
- *Events by Severity*



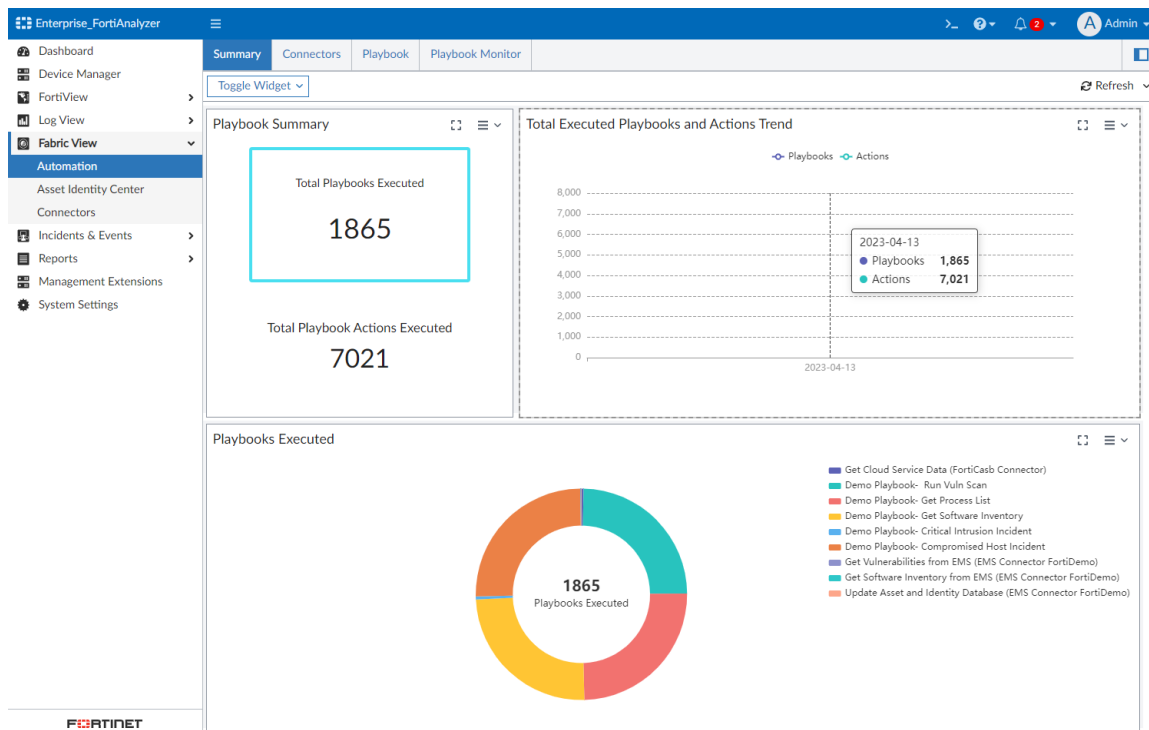
- *Top 10 Events by Handler*

**Incidents**

This dashboard includes the following widgets:

- *Total Incidents*
- *Unsolved Incidents*
- *Incidents Timeline*

To configure FortiSoC playbooks, go to *Fabric View > Automation*.



*Fabric View > Automation* includes the following:

<b>Summary</b>	View playbook performance in a dashboard. This includes widgets for total playbooks, playbooks executed, and an actions trend. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Connectors</b>	View the status of available connectors supported for playbook automation. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Playbook</b>	Configure and manage playbooks. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Playbook Monitor</b>	View playbook jobs in a table view. For more information, see the <a href="#">FortiAnalyzer Administration Guide</a> .

## Notifications for new Outbreak Alerts - 7.4.1



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [Outbreak Alerts](#)

When new Outbreak Alerts are received, GUI notifications are added in the banner, ensuring timely notification for administrators.

In the *Outbreak Alerts* pane, the Outbreak Alerts can now be sorted by *Date* or *Severity*, allowing for easy browsing and retrieval based on these criteria. A "New" tag is also added to alerts received in the current month to distinguish them from previous alerts.

For example, see the image below.

Use the tree menu in the sidebar to expand and browse the list of alerts.

After refreshing the pane, you will no longer see the *New* tag.

The screenshot shows the FortiAnalyzer 7.4.0 interface. On the left, the sidebar menu is open, showing the 'Incidents & Events' section with 'Outbreak Alerts' selected. The main pane displays 'OUTBREAK ALERTS' with a search bar and a 'Group by' dropdown set to 'Date'. A calendar view shows alerts for July 2023, including 'Microsoft Office and Windows HTML RCE Vulnerability', 'SolarView Compact Comm', and 'Apache RocketMQ Remote'. The main content area shows the details for the 'Microsoft Office and Windows HTML RCE Vulnerability' alert, including a link to a Microsoft security blog post and a background section about the Storm-0978 threat actor.

To group alerts in the sidebar by severity instead of *Date*, select the *Severity* radio button.

The screenshot shows the FortiAnalyzer 7.4.0 interface with the 'Outbreak Alerts' pane. The 'Group by' dropdown is now set to 'Severity'. The calendar view shows alerts grouped by severity, with 'Critical' alerts listed, including 'Progress MOVEit Transfer SQL I', '3CX Supply Chain Attack', 'Outbreak Alert- 2022 Annual R', 'Hive Ransomware', 'CISA Top 20 Vulnerabilities', 'Microsoft Exchange ProxyNotSI', 'Apache Log4j2 Vulnerability', 'VMWare Spring4Shell Vulnerab', 'Microsoft PrintNightmare Vulne', 'Kaseya VSA Attack', 'F5 BIG-IP & BIG-IQ Vulnerabilit', 'Microsoft Exchange Server RCE', and 'SolarWinds Orion Attack'. The main content area remains the same, showing details for the 'Microsoft Office and Windows HTML RCE Vulnerability' alert.

# Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- [Logging on page 16](#)
- [Log Forwarding on page 30](#)
- [Reports on page 34](#)
- [Others on page 46](#)

## Logging

This section lists the new features added to FortiAnalyzer for logging:

- [FortiAnalyzer supports FortiWeb Cloud attack logs on page 16](#)
- [Support parsing and addition of third-party application logs to the SIEM DB on page 17](#)
- [Per-ADOM log rate on page 22](#)
- [Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 on page 24](#)
- [Logging support for FortiCASB 7.4.1 on page 26](#)
- [Logging support for FortiPAM 7.4.1 on page 28](#)
- [Logging support for FortiToken Cloud 7.4.1 on page 29](#)

## FortiAnalyzer supports FortiWeb Cloud attack logs

FortiAnalyzer now supports FortiWeb Cloud attack logs, and additional event/attack log fields have been added.

After adding and authorizing a FortiWeb Cloud device in FortiAnalyzer, you can view Attack and Event logs from this device in *Log View*.

### To view FortiWeb Cloud logs in FortiAnalyzer:

1. In *Device Manager*, add and authorize the FortiWeb Cloud device.
2. To view logs from the FortiWeb Cloud device, go to *Log View > Log Browse*.

Add Filter		All Devices		Last 1 Day		Display Delete Download Import			
<input type="checkbox"/>	#	Device Name	Serial Number	VDOM	Type	File Name	From	To	Size
<input type="checkbox"/>	1	FVBCLD3920584167	FVBCLD3920584167	root	Attack	alog.log	2023-01-30 16:10:21	2023-02-02 10:11:46	17.3k
<input type="checkbox"/>	2	FVBCLD3920584167	FVBCLD3920584167	root	Event	elog.log	2023-01-30 16:10:21	2023-02-02 10:25:37	11.2k
<input type="checkbox"/>	3	FVBCLD3546102879	FVBCLD3546102879	root	Attack	alog.log	2023-01-30 16:10:20	2023-02-02 10:11:53	23.0k
<input type="checkbox"/>	4	FVBCLD3546102879	FVBCLD3546102879	root	Event	elog.log	2023-01-30 16:10:19	2023-02-02 10:25:40	12.6k
<input type="checkbox"/>	5	.self	FAZVMSTM22000868	leo-FWB-CLD	App Events	rlog.log	2023-01-29 17:44:40	2023-02-02 10:14:49	4.1k

You can also go to *Log View > FortiWeb > Attack*. This includes FortiWeb Cloud attack logs, as well as four new fields:

- *user\_id*, which corresponds to the *User ID* column
- *app\_id*, which corresponds to the *Application ID* column
- *app\_name*, which corresponds to the *Application Name* column
- *app\_domain*, which corresponds to the *Application Domain* column

See an example of *Log View > FortiWeb > Attack* below.

All FortiWeb - Last 1 Hour - 09:30:50 To 10:30:49											
#	Date/Time	Device ID	Source Name	Action	HTTP URL	HTTP Host	Message	Application Name	Application Domain	Application ID	Login User Name
1	10:11:44	FVBCLD354...		Block	none	none	IP Protection...	WestWind DI	www.westwinddi.com	1082477833	Unknown
2	10:11:43	FVBCLD392...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown
3	10:11:42	FVBCLD392...		Monitor	/SeguroDeAu...	autos.elpotosi...	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown
4	10:11:41	FVBCLD392...		Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown
5	10:11:40	FVBCLD354...		Block	none	none	IP Protection...	WestWind DI	www.westwinddi.com	1082477833	Unknown
6	10:11:39	FVBCLD354...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown
7	10:11:38	FVBCLD392...		Monitor	/SeguroDeAu...	autos.elpotosi...	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown
8	10:11:37	FVBCLD354...		Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown
9	10:11:36	FVBCLD354...		Block	none	none	IP Protection...	WestWind DI	www.westwinddi.com	1082477833	Unknown
10	10:11:35	FVBCLD392...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown

Finally, you can also go to *Log View > FortiWeb > Event*. This includes FortiWeb Cloud event logs, as well as five new fields:

- *user\_id*, which corresponds to the *User ID* column
- *login\_user*, which corresponds to the *User* column
- *app\_id*, which corresponds to the *Application ID* column
- *app\_name*, which corresponds to the *Application Name* column
- *app\_domain*, which corresponds to the *Application Domain* column

See an example of *Log View > FortiWeb > Event* below.

All FortiWeb - Last 1 Hour - 09:31:51 To 10:31:50											
#	Date/Time	Device ID	Level	Action	Message	Application Domain	Application ID	Application Name	Application ID	Application Name	User
1	10:25:32	FVBCLD3546102879	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...
2	10:25:31	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...
3	10:25:30	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	9462702209	Agent Etimad	1245460@qq.c...
4	10:25:29	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	NULL	NULL	1245460@qq.c...
5	10:25:28	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...
6	10:25:27	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...
7	10:25:26	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	9462702209	Agent Etimad	1245460@qq.c...
8	10:25:25	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	NULL	NULL	1245460@qq.c...
9	10:25:24	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...
10	10:25:23	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	2623501487	MyApp10	1245460@qq.c...

## Support parsing and addition of third-party application logs to the SIEM DB



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [SIEM log parsers](#)

FortiAnalyzer supports parsing and addition of third-party application logs to the SIEM DB.

There are two types of log parsers:

- Predefined parsers
- Custom parsers

You can find predefined SIEM log parsers in *Incidents & Events > Log Parser > Log Parsers*. There are predefined parsers for all fabric related Fortinet products. Predefined Apache and Nginx web server log parsers have also been added to this list of predefined SIEM log parsers.

The configuration of each SIEM log parser (predefined and custom) is specific to the ADOM that you are in. Any changes to an existing parser or any newly added parsers will only affect the ADOM that the action was completed in. Ensure you are in the correct ADOM when working with log parsers.

The following information is provided in this topic:

- [To view the log parsers: on page 18](#)
- [The Apache web server log parser: on page 19](#)

- The Nginx web server log parser: on page 19
- To import a custom log parser: on page 20
- To validate if the original logs can be parsed: on page 21
- To assign devices to a log parser: on page 21

### To view the log parsers:

1. In **Incidents & Events > Log Parser > Log Parsers**, select **Show Predefined** and/or **Show Custom** to show the available log parsers in the table view.

Each predefined log parser is assigned a default *Application* and *Category*. Custom log parsers are assigned a default *Application* and *Category* when they are imported.

The **#** column is the priority of each Siem Log\_Parser from highest (1) to lowest. By default, newly imported custom log parsers are assigned the lowest priority. To change the priority, click the left edge of the row and drag and drop it to the desired area in the table. See below.

#	Name	Application	Category	Status
1	Apache Log Parser	Apache Web Server	Web Server	Enabled
2	FortiADC Log Parser	FortiADC	Fortinet Device	Enabled
3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	Enabled
4	FortiCache Log Parser	FortiCache	Fortinet Device	Enabled
5	FortiClient Log Parser	FortiClient	Fortinet Device	Enabled
6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	Enabled
7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	Enabled
8	FortiEDR Log Parser	FortiEDR	Fortinet Device	Enabled
9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	Enabled
10	FortiGate Log Parser	FortiGate	Fortinet Device	Enabled

2. Double-click a log parser in the table view to display all related SIEM logs. Alternatively, you can select the checkbox for the log parser and click **View Logs**.

#	Date/Time	Data Source ID	Event Message
26	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the performance threshold.)
27	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the performance threshold.)
28	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the performance threshold.)
29	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the performance threshold.)
30	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
31	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
32	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
33	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
34	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
35	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
36	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
37	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
38	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
39	16:51:02	FGVM02TM23000735	FortiGuard hostname unresolvable(unable to resolve FortiGuard hostname)
40	16:51:02	FG101E4Q17003922	Automation sfttch triggered(utttch-FortiAnalyzer Connection Down is triggered.)
41	16:51:02	FG101E4Q17003922	Automation sfttch triggered(utttch-FortiAnalyzer Connection Down is triggered.)
42	16:51:02	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performance threshold.)
43	16:51:02	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
44	16:51:02	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
45	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
46	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
47	16:51:02	FWF61ETK18005359	SDWAN SLA information(Health Check SLA status.)
48	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
49	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
50	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)

3. Select the checkbox for one or more log parsers in the table to perform an action from the toolbar. For example, you can **Export** in JSON format, **Enable**, **Disable**, **Delete**, or **Validate** the log parsers. Some actions will be unavailable if they cannot be performed on the selected log parser(s).

- You cannot **Disable** a log parser if it is assigned and in use.
- You cannot **Delete** predefined log parsers. They can only be disabled.

- You cannot perform the *Validate* action on more than one parser at a time.

#	Name	Application	Category	Status
1	Apache Log Parser	Apache Web Server	Web Server	Enabled
2	FortiADC Log Parser	FortiADC	Fortinet Device	Enabled
3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	Enabled
4	FortiCache Log Parser	FortiCache	Fortinet Device	Enabled
5	FortiClient Log Parser	FortiClient	Fortinet Device	Enabled
6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	Enabled
7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	Enabled
8	FortiEDR Log Parser	FortiEDR	Fortinet Device	Enabled
9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	Enabled
10	FortiGate Log Parser	FortiGate	Fortinet Device	Enabled

### The Apache web server log parser:

Go to *Incidents & Events > Log Parser > Log Parsers* to find the Apache Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.

#	Name	Application	Category	Status
1	Apache Log Parser	Apache Web Server	Web Server	Enabled
2	FortiADC Log Parser	FortiADC	Fortinet Device	Enabled
3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	Enabled
4	FortiCache Log Parser	FortiCache	Fortinet Device	Enabled
5	FortiClient Log Parser	FortiClient	Fortinet Device	Enabled
6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	Enabled
7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	Enabled
8	FortiEDR Log Parser	FortiEDR	Fortinet Device	Enabled
9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	Enabled
10	FortiGate Log Parser	FortiGate	Fortinet Device	Enabled

The Apache logs are also parsed in *Log View > Fabric > All*. You can filter by Data Parser Name = Apache Log Parser.

#	Date/Time	Data Source ID	Event Message
1	10:31:23	SYSLOG-0A029559	10.2.0.250 - - [29/Mar/2023:10:31:05 -0700] "GET /favicon.ico HTTP/1.1" 404 (Not Found) "http://10.2.149.8:8080/..."
2	10:30:23	SYSLOG-0A029559	10.2.0.250 - - [29/Mar/2023:10:30:13 -0700] "GET /favicon.ico HTTP/1.1" 404 (Not Found) "http://10.2.149.8:8080/..."
3	10:30:23	SYSLOG-0A029559	/10.2.149.89/"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36"
4	00:00:10	SYSLOG-0A029559	AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.2.149.8
5	00:00:10	SYSLOG-0A029559	[Wed Mar 29 00:00:01.121897 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00049: Core
6	03:27:00:00	SYSLOG-0A029559	[Mon Mar 27 00:00:09.403064 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00049: Core
7	03:27:00:00	SYSLOG-0A029559	[Mon Mar 27 00:00:09.403064 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00049: Core
8	03:26:00:00	SYSLOG-0A029559	AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.2.149.8
9	03:26:00:00	SYSLOG-0A029559	[Sun Mar 26 00:00:11.574064 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00493: Core
10	03:25:00:00	SYSLOG-0A029559	[Sat Mar 25 00:00:16.155107 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00094: Comm
11	03:25:00:00	SYSLOG-0A029559	[Sat Mar 25 00:00:16.155107 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00489: Comm
12	03:24:00:00	SYSLOG-0A029559	[Fri Mar 24 00:00:06.745261 2023] [mpm_eventnotice] [pid 2904315:tid 140086293559168] AH00094: Comm

### The Nginx web server log parser:

Go to *Incidents & Events > Log Parser > Log Parsers* to find the Nginx Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.

#	Name	Application	Category	Status
16	FortiNDR Log Parser	FortiNDR	Fortinet Device	Enabled
17	FortiProxy Log Parser	FortiProxy	Fortinet Device	Enabled
18	FortiSOAR Log Parser	FortiSOAR	Fortinet Device	Enabled
19	FortiSandbox Log Parser	FortiSandbox	Fortinet Device	Enabled
20	FortiSwitch Log Parser	FortiSwitch	Fortinet Device	Enabled
21	FortiWeb Log Parser	FortiWeb	Fortinet Device	Enabled
22	Nginx Log Parser	Nginx Web Server	Web Server	Enabled
23	System Log Parser	Generic System	Generic System	Enabled
24	Ubuntu Syslog Parser	Ubuntu	Ubuntu System	Enabled
25	Windows XML Event Log Parser	Windows	Windows System	Enabled

The Nginx logs are also parsed in *Log View > Fabric > All*. You can filter by Data Parser Name = Nginx Log Parser.

#	Date/Time	Data Source ID	Event Message
1	10:30:14	SYSLOG-0A029558	10.2.0.250 - [29/Mar/2023:10:30:02 -0700] "GET /favicon.ico HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
2	10:30:14	SYSLOG-0A029558	10.2.0.250 - [29/Mar/2023:10:30:02 -0700] "GET / HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
3	03:23:16:17	SYSLOG-0A029558	10.2.0.250 - [23/Mar/2023:16:16:54 -0700] "GET / HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
4	03:23:16:17	SYSLOG-0A029558	10.2.0.250 - [23/Mar/2023:16:16:54 -0700] "GET / HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
5	03:23:08:54	SYSLOG-0A029558	10.2.0.250 - [23/Mar/2023:08:54:05 -0700] "GET /favicon.ico HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
6	03:23:08:54	SYSLOG-0A029558	10.2.0.250 - [23/Mar/2023:08:54:04 -0700] "GET / HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
7	03:23:08:54	SYSLOG-0A029558	10.2.0.250 - [23/Mar/2023:08:54:04 -0700] "GET / HTTP/1.1" 304 0 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

## To import a custom log parser:

- In *Incidents & Events > Log Parser > Log Parsers*, click *Import*.  
The *Import Log Parser* dialog displays.
- Drag and drop or select the log parser.  
The log parser must be in the correct format as a JSON file to meet the requirements checked during the import.
- Click *OK*.  
Once added, the custom log parser will be included in the table view when *Show Custom* is selected.

#	Name	Application	Category	Status
26	Custom Log Parser	FortiADC	Fortinet Device	Enabled



## To validate if the original logs can be parsed:

1. In *Incidents & Events > Log Parser > Log Parsers*, select the checkbox for a log parser.
2. Click *Validate*.  
The *Validate Log Parser* pane opens.
3. Enter a log to validate and click *Validate*.

A *Parse Result* will display in the same pane.

Validate FortiGate Log Parser

Enter a log to validate

```
logseq=2415036964254525 time=2023-03-24 17:03:38 devid=FG101E4Q17000739 uid=root date=2023-03-24 time=17:03:32 logid=0000000020
type=traffic subtype=forward level=notice eventtime=1679702614205080064 tz=-0700 srcip=192.168.1.119 srcport=2577 srcint=lan srcintrole=lan
dstip=10.2.60.103 dstport=514 dstint=mgmt dstintrole=lan srcuid=915fce5c-ca67-51e7-f5d6-18986449647b dsuid=1782a2b6-bdcf-51e7-c24e-
fcd37122304d sessionid=2196072 proto=6 action=accept polycid=6 policytype=policy poluid=430f78f0-6e79-51ec-9b95-98d9d18464b
service=tcp 514 dstcountry=Reserved srccountry=Reserved transp=nat transp=10.2.60.119 transport=2577 duration=76219 sentbyte=36963127
rcvbyte=3071930 sentpkt=58200 rcvpkt=35631 appcat=unscanned sentdrt=1305998 csdrt=12582 masterdrtmac=0cc4:7ada:13:50
dstmac=0cc4:7ada:13:50 dstserver=1 dtime=2023-03-24 17:03:32 time_t=1679702618 offset_id=0
```

Validate

Parse Result

Matched

Order Parsed Log

```
adom_oid = 3 time = 1679702670 loguid = 1804289383 data_parsername = FortiGate Log Parser
data_sourceid = FG101E4Q17000739 data_sourceidname = FG101E4Q17000739 root data_sourceidtype = FortiGate
data_timestamp = 2023-03-24 app_cat = unscanned app_service = tcp/514 dst_geo = Reserved dst_intf = mgmtlan
dst_ip = 10.2.60.103 dst_mac = 0cc4:7ada:13:50 dst_port = 514 event_action = accept event_id = 20 event_severity = notice
event_subtype = forward event_type = traffic host_ip = 192.168.1.119 host_location = Reserved
host_uid = 915fce5c-ca67-51e7-f5d6-18986449647b net_proto = 6 net_rcvpkts = 35631 net_rcvbytes = 3071930
net_sentbytes = 36963127 net_sentpkts = 58200 net_sessionduration = 76219 net_sessionid = 2196072 src_geo = Reserved
src_intf = lanlan src_ip = 192.168.1.119 src_natip = 10.2.60.119 src_natport = 2577 src_port = 2577
```

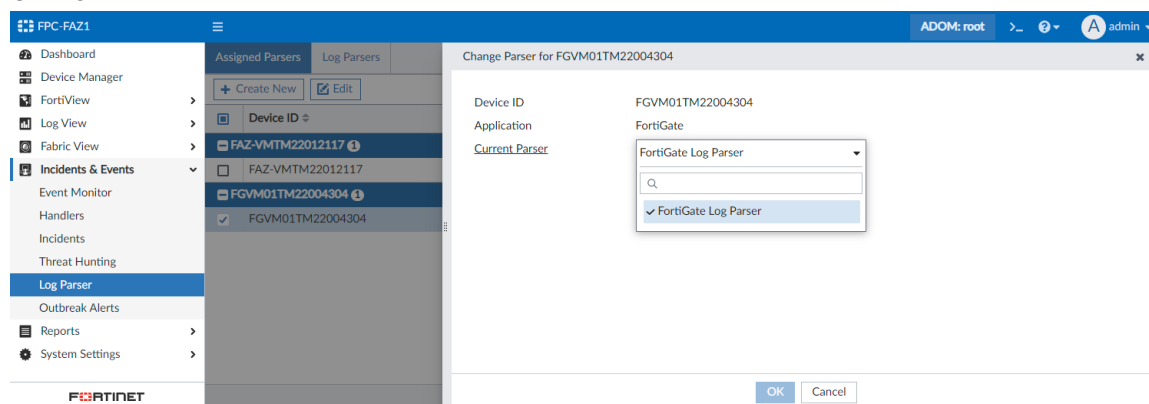
## To assign devices to a log parser:

1. Go to *Incidents & Events > Log Parser > Assigned Parsers*.  
The existing log parser assignments display in a table view.

Device ID	Application	Assigned Parser
FAZ-VMTM22012117	FortiAnalyzer	FortiManager/FortiAnalyzer Log Parser - FortiAnalyzer
FGVM01TM22004304	FortiGate	FortiGate Log Parser

2. Select the checkbox for an existing log parser assignment and click *Edit*.  
Alternatively, you can click *Create New* to create a new log parser assignment.  
The *Change Parser* pane displays.
3. From the *Current Parser* dropdown, select the log parser to assign the device/application to.

## 4. Click OK.



## Per-ADOM log rate

To better fit multi-tenancy deployment, FortiAnalyzer provides a per-ADOM log rate that the administrator can monitor to prevent one ADOM/customer from impacting the stability of the entire unit.

An additional diskquota log has been introduced to inform the administrator when an ADOM reaches the configured quota threshold.

### To view the logs in the GUI:

A log message for ADOM performance statistics (log rate) is added to both FortiAnalyzer Event logs and Application logs. FortiAnalyzer Event logs will generate this message for all ADOMs, while Application logs will generate this message for the current ADOM only.

For example, see the below log messages in *Log View > FortiAnalyzer > Event*:

#	↓Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On	Changes
12	17:34:39	FAZ-VMTM22011	system	system	System performance status: log rate low (0%), lograte=67/sec.	Perf stats	Local system	Show system performance stats.
13	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDeceptor performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
14	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAnalyzer performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
15	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewall performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
16	17:29:48	FAZ-VMTM22011	system	system	Adom FortiProxy performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
17	17:29:48	FAZ-VMTM22011	system	system	Adom Syslog performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
18	17:29:48	FAZ-VMTM22011	system	system	Adom FortiManager performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
19	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAuthenticator performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
20	17:29:48	FAZ-VMTM22011	system	system	Adom FortiSandbox performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
21	17:29:48	FAZ-VMTM22011	system	system	Adom root performance status: lograte=76/sec	Perf stats	Local system	Show adom performance stats.
22	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
23	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDoS performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
24	17:29:48	FAZ-VMTM22011	system	system	Adom FortiWeb performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
25	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCache performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
26	17:29:48	FAZ-VMTM22011	system	system	Adom FortiMail performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
27	17:29:48	FAZ-VMTM22011	system	system	Adom FortiClient performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
28	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewallCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.

For example, see the below log messages in *Log View > FortiAnalyzer > Application*:

eFAZ-227

Member

ADOM: root

>

1

admin

Dashboard

Device Manager

FortiView

Log View

Fabric

FortiGate

FortiClient

FortiSandbox

FortiAnalyzer

Log Browse

Log Group

Fabric View

Incidents & Events

Reports

System Settings

Event

Application

All Devices ▾ Last 12 Hours ▾ 06:10:26 To 18:10:25

Event Type = perf-stats ×

#	↓Date/Time	Device ID	User	Sub Type	Event Type	Action	Message	Description
1	17:29:48	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=76/sec	Adom performance statistics notice
2	16:29:48	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=67/sec	Adom performance statistics notice
3	15:29:48	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=60/sec	Adom performance statistics notice
4	14:29:48	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=73/sec	Adom performance statistics notice
5	13:29:48	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=59/sec	Adom performance statistics notice
6	12:15:59	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=46/sec	Adom performance statistics notice
7	11:15:59	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=58/sec	Adom performance statistics notice
8	09:25:40	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=54/sec	Adom performance statistics notice
9	08:25:40	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=55/sec	Adom performance statistics notice
10	07:25:40	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=61/sec	Adom performance statistics notice
11	06:25:40	FAZ-VM2M22011	system	system	perf-stats	Stats	Adom root performance status: lograte=64/sec	Adom performance statistics notice

A log message is also added for ADOM archive usage to Local Application Logs. See below example taken from *Log View > FortiAnalyzer > Application*:

#	↓Date/Time	Device ID	Sub Type	User	Message	Event Type	Description
1	2023-03-21 20:37:29	FAZ-VM2M23003736	diskquota	system	Disk usage for Adom Lab is approaching the delete threshold 90% of total 50. disk-usage		Disk quota warning
2	2023-03-21 20:36:48	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=1056/sec	perf-stats	Adom performance s
3	2023-03-21 20:31:48	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=59/sec	perf-stats	Adom performance s
4	2023-03-21 20:31:40	FAZ-VM2M23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009] logging-status		Device offline
5	2023-03-21 20:23:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
6	2023-03-21 20:18:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
7	2023-03-21 20:13:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
8	2023-03-21 20:08:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=58/sec	perf-stats	Adom performance s
9	2023-03-21 20:03:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
10	2023-03-21 19:58:56	FAZ-VM2M23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=52/sec	perf-stats	Adom performance s
11	2023-03-21 19:58:47	FAZ-VM2M23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009] logging-status		Device offline

## To set the interval for the ADOM performance statistics logs:

CLI configuration is added for the interval time to log performance state.

In the FortiAnalyzer CLI, enter the following command:

```
config system locallog setting
  set log-interval-adom-perf-stats <integer>
end
```

For the `log-interval-adom-perf-stats` setting, enter the interval in minutes. The range should be 5-2880. Enter 0 to disable the logs.

## Example logs:

Event log message for ADOM performance statistics (log rate):

```
id=7231962960615178247 bid=865533 dvid=1040 itime=1683822591 euid=1 epid=1 dsteuid=1
dstepid=1 log_id="0001010093" subtype="system" type="event" level="notice"
time="09:29:51" date="2023-05-11" user="system" action="Stats" msg="Adom root
performance status: lograte=54/sec" userfrom="system" desc="Adom performance
statistics notice" operation="Perf stats" performed_on="Local system" changes="Show
adom performance stats." lograte=54 logratelimit=0 tz="-0700" devid="FAZ-VM2M22011553"
devname="eFAZ-227"
```

Application log message for ADOM performance statistics (log rate):

```
id=7207521362594958664 bid=101707 dvid=1059 itime=1678131838 euid=1 epid=1 dsteuid=1
dstepid=1 vd="fortinet" logid="220004" type="appevent" subtype="system"
eventtype="perf-stats" action="Stats" level="notice" date="2023-03-06" time="11:43:58"
user="system" user_from="system" desc="Adom performance statistics notice" msg="Adom
```

```
fortinet performance status: log rate low (0%), lograte=49/sec" tz="-0800"
adom="fortinet" operation="Perf stats" lograte=49 performed_on="Local system"
changes="Show adom performance stats." logratelimit=0 devid="FAZ-VMTM23003360"
devname="eFAZ-54"
```

#### Log message for ADOM archive usage:

```
id=7207519107737128256 bid=100933 dvid=1059 itime=1678131313 euid=1 epid=1 dsteuid=1
dstepid=1 vd="fortinet" logid="220003" type="appevent" subtype="diskquota"
eventtype="disk-usage" level="warning" date="2023-03-06" time="11:35:14" user="system"
user_from="system" desc="Disk quota warning" msg="Disk usage for Adom fortinet is
approaching the delete threshold 90% of total 50.0MB. Archive Usage at 196.7%(29.5MB)
and Analytics Usage at 41.6%(14.6MB)." tz="-0800" adom="fortinet" diskusage=88
devid="FAZ-VMTM23003360" devname="eFAZ-54"
```

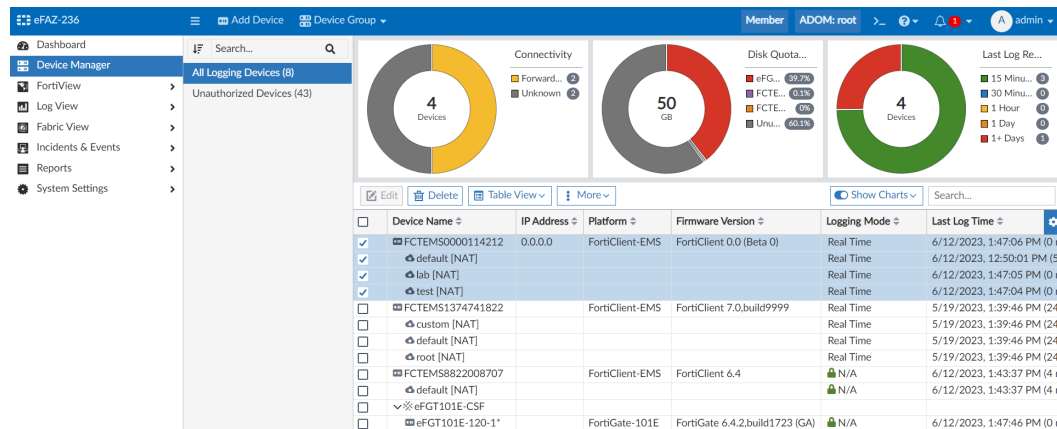
## Support EMS multitenancy via FortiAnalyzer ADOMs - 7.4.1

With FortiClient EMS multitenancy, you can create multiple sites, providing granular access to different sites and separating endpoint data and configurations.

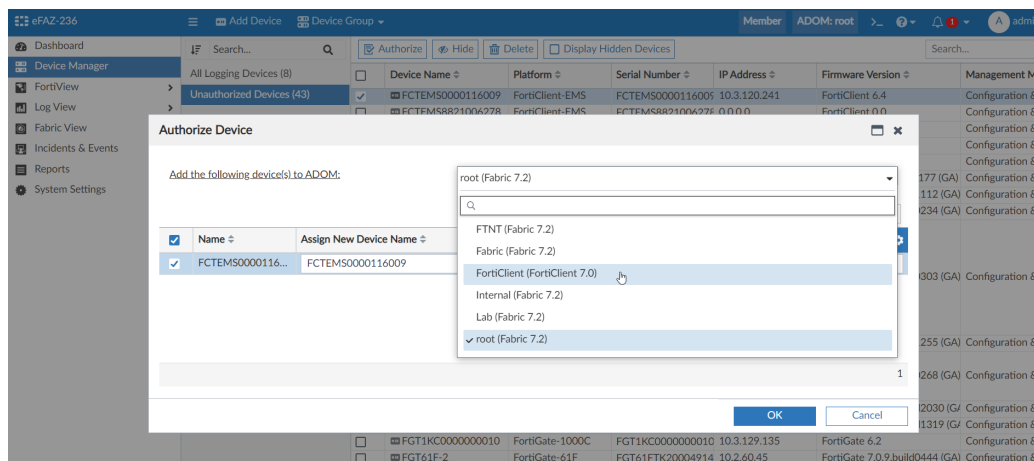
FortiAnalyzer has added support to EMS multitenancy by providing the following:

- Each log is mapped to its corresponding site using the `vd` log field
- EMS sites can be assigned to different FortiAnalyzer ADOMs

EMS logs (with multiple FCT logs) can be received by FortiAnalyzer directly with required fields added.



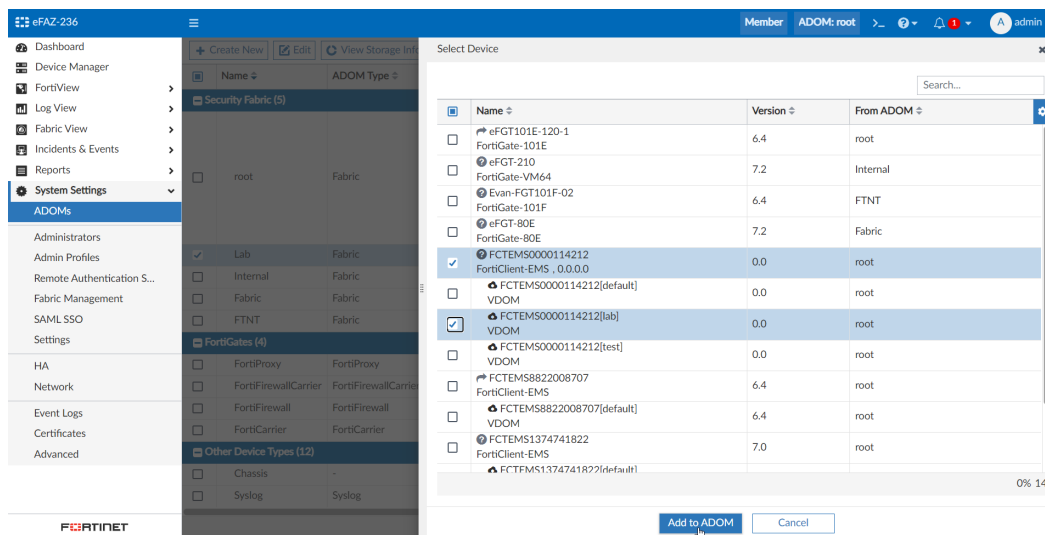
FortiClient can be promoted into Fabric ADOM or FortiClient ADOM in FortiAnalyzer.



The FortiClient logs from multitenancy logs can be converted to `vd=siteName` when receiving logs.

#	Date/Time	Registered to Device	Virtual Domain	Site	User	Sub Type	Host Name	Message
1	13:54:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
2	13:52:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
3	13:51:47	FCTEM50000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
4	13:51:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
5	13:49:47	FCTEM50000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
6	13:49:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
7	13:48:47	FCTEM50000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
8	13:48:13	FCTEM50000114212	default	default	fc12	update	QA2-PC	Update was successful
9	13:48:09	FCTEM50000114212	default	default	fc12	update	QA2-PC	Update was successful to the given version for the
10	13:48:09	FCTEM50000114212	default	default	fc12	update	QA2-PC	Update was successful to the given version for the
11	13:48:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
12	13:46:47	FCTEM50000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
13	13:46:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
14	13:45:01	FCTEM50000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ

The multitenancy logs can be assigned to different ADOMs based on its VDOM when the *ADOM Mode* is set to *Advanced*.



Two new fields are added to FortiClient logs:

- vd
- regdevname

The FortiClient logs can be filtered by these fields in *Log View*. For example, see below.

#	Date/Time	Registered to Device	Virtual Domain	User	Sub Type	Host Name	Message
1	13:58:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
2	13:57:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
3	13:56:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
4	13:56:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
5	13:55:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
6	13:55:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
7	13:54:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
8	13:54:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
9	13:52:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
10	13:52:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
11	13:51:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
12	13:51:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
13	13:49:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
14	13:49:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
15	13:48:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
16	13:48:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
17	13:46:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ

## Logging support for FortiCASB - 7.4.1

FortiAnalyzer can now receive, store, and display logs from authorized FortiCASB devices in *Log View*.

### To configure FortiCASB logging to FortiAnalyzer:

1. In the FortiCASB GUI, go to *Overview > Fabric Integration > Add New FortiAnalyzer*.
2. Configure the following settings for the FortiAnalyzer device and click *Add New FortiAnalyzer*:
  - *Device Name*
  - *Device IP Address*
  - *Device Serial Number*

FortiCloud Services Support

FortiCASB Version 23.2.b

Overview / Fabric Integration / Add New FortiAnalyzer

Add New FortiAnalyzer

1 Fill In Info 2 Done

Device Name \*

TestDevice

Device IP Address \*

10.200.7.175

Device Serial Number \*

FAZ-VMTM

Alert To Be Sent To FortiAnalyzer \*

☐ Data Analysis

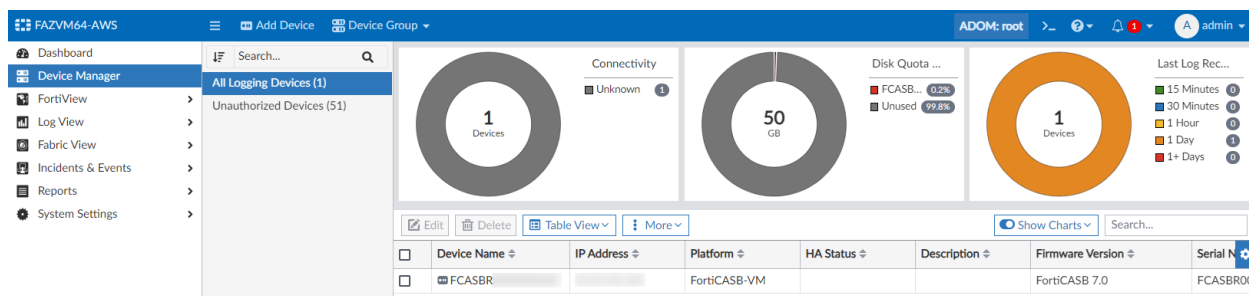
Add New FortiAnalyzer Cancel

3. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.

The FortiCASB displays in the *Unauthorized Devices* list.

4. Select the FortiCASB device and click *Authorize*.

The FortiCASB device now displays in *All Logging Devices* list.



The FortiCASB logs display in *Log View > FortiCASB*.

FAZVM64-AWS

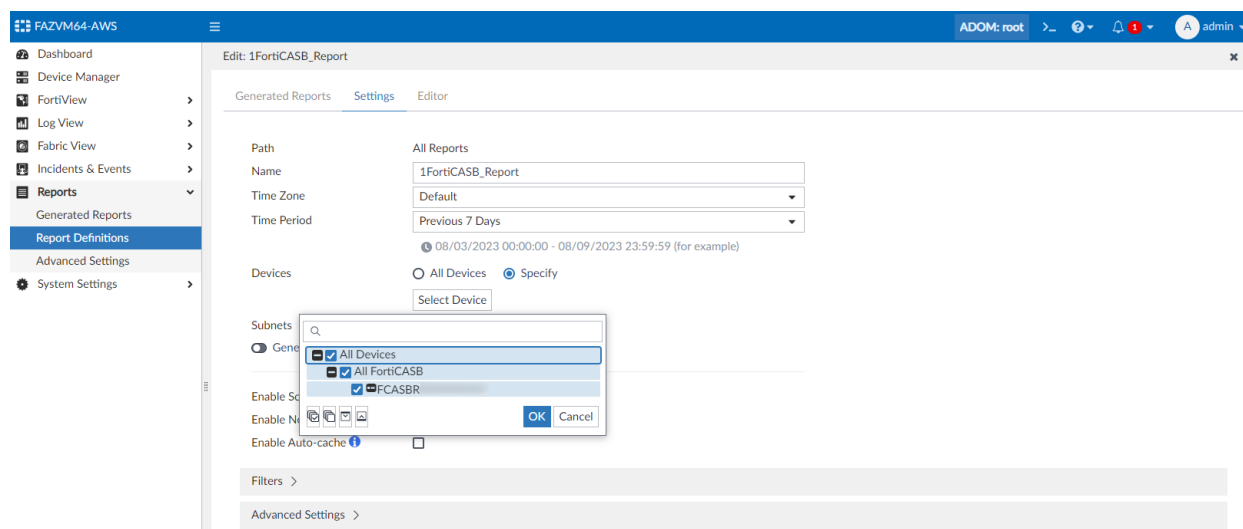
Dashboard Device Manager FortiView Log View Fabric View Incidents & Events Reports System Settings

Data Leak Prevention

FCASBR Last 1 Day Aug 09 To Aug 10

#	Date/Time	Device ID	Type	Sub Type	Level	Source IP	Policy ID
1	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288554
2	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288590
3	08-09 19:18	FCASBR	dlp	null	4		288480
4	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288588
5	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288560
6	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288550
7	08-09 19:18	FCASBR	dlp	null	4		288479
8	08-09 19:18	FCASBR	dlp	Personal Identity In	4		288571
9	08-09 19:18	FCASBR	dlp	null	4		288484

The FortiCASB device can now be used in *Reports*.

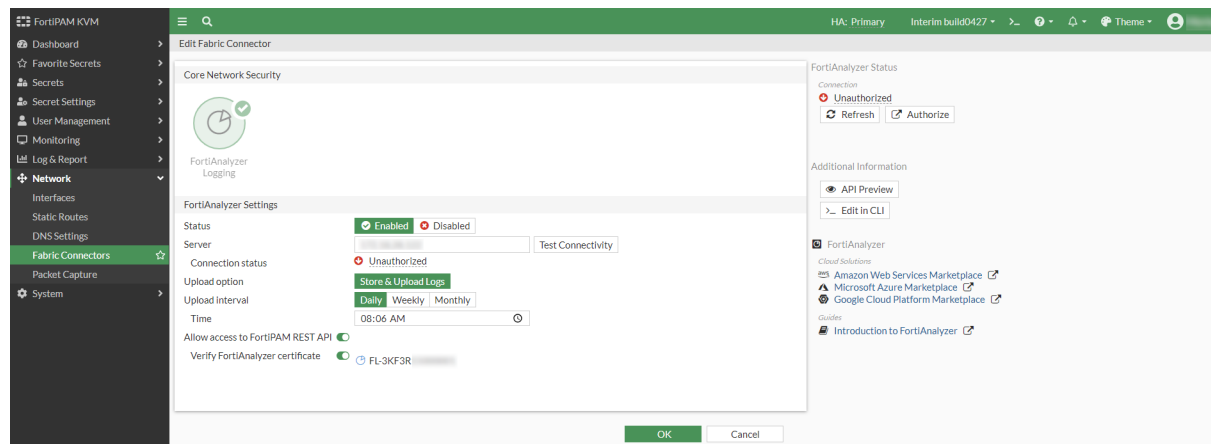


## Logging support for FortiPAM - 7.4.1

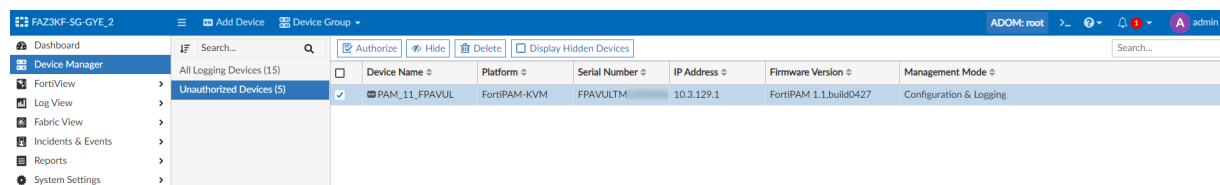
FortiAnalyzer now supports logs from FortiPAM.

**To configure FortiPAM logging to FortiAnalyzer:**

1. In the FortiPAM GUI, go to *Network > Fabric Connectors*, and edit *FortiAnalyzer Logging*. In the *Server* field, enter the FortiAnalyzer IP address.

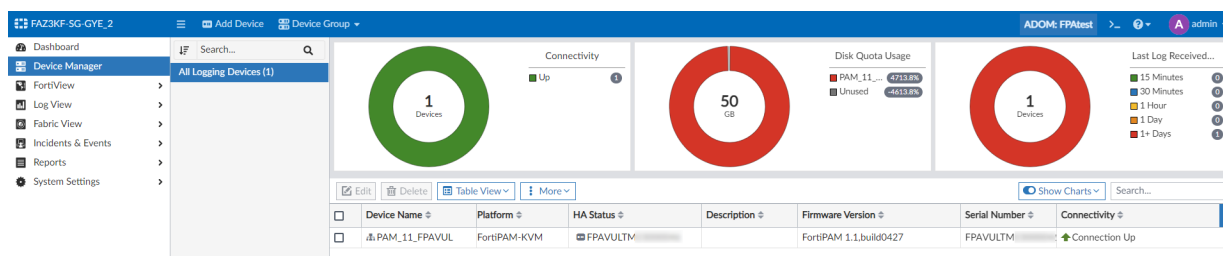


2. In the FortiAnalyzer GUI root ADOM, go to *Device Manager > Unauthorized Devices*. Select the FortiPAM device and click *Authorize*.



The FortiPAM device is now authorized in *Device Manager*.





3. To view logs from the FortiPAM device, go to *Log View > FortiPAM*.

The screenshot shows the FortiAnalyzer Log View for FortiPAM. The left sidebar is the same as the dashboard. The main area displays a table of log entries with columns: #, Date/Time, Device ID, Type, Sub Type, Protocol, Log ID, Virtual Domain, Destination IP, Session ID, Device Name, Device Time, WAN In, and WAN Out. The table contains 9 entries, all of type 'traffic' and 'forward'.

#	Date/Time	Device ID	Type	Sub Type	Protocol	Log ID	Virtual Domain	Destination IP	Session ID	Device Name	Device Time	WAN In	WAN Out
1	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057766	FPAVULTM	2019-06-04 1		
2	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057760	FPAVULTM	2019-06-04 1		
3	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057765	FPAVULTM	2019-06-04 1		
4	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057762	FPAVULTM	2019-06-04 1		
5	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057761	FPAVULTM	2019-06-04 1		
6	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057763	FPAVULTM	2019-06-04 1		
7	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057758	FPAVULTM	2019-06-04 1		
8	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057757	FPAVULTM	2019-06-04 1		
9	06-22 09:44	FPAVULTM	traffic	forward	17	0000000013	root		3666057752	FPAVULTM	2019-06-04 1		

You can create a FortiPAM report in FortiAnalyzer.

The screenshot shows the FortiAnalyzer Report Definitions page. The left sidebar is the same as the dashboard. The main area displays a table of reports with columns: Report Name, Format, Report Execution Time, Data Range, Devices, and Status. The table contains one entry: FortiPAM\_report1-2023-07-10-1639-0700\_49703, HTML PDF XML CSV JSON, 2023-07-10 16:39:50 PDT, 2023-04-01 00:00:00 - 2023-07-09 23:59:59 PDT, PAM\_11\_FPAVUL[root], and 3s.

Report Name	Format	Report Execution Time	Data Range	Devices	Status
FortiPAM_report1-2023-07-10-1639-0700_49703	HTML PDF XML CSV JSON	2023-07-10 16:39:50 PDT	2023-04-01 00:00:00 - 2023-07-09 23:59:59 PDT	PAM_11_FPAVUL[root]	3s

## Logging support for FortiToken Cloud - 7.4.1

FortiAnalyzer can now receive, store, and display logs from authorized FortiToken Cloud devices in *Log View*.

To configure FortiToken Cloud logging on FortiAnalyzer:

1. Configure the FortiToken Cloud device to send logs to FortiAnalyzer.
2. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.

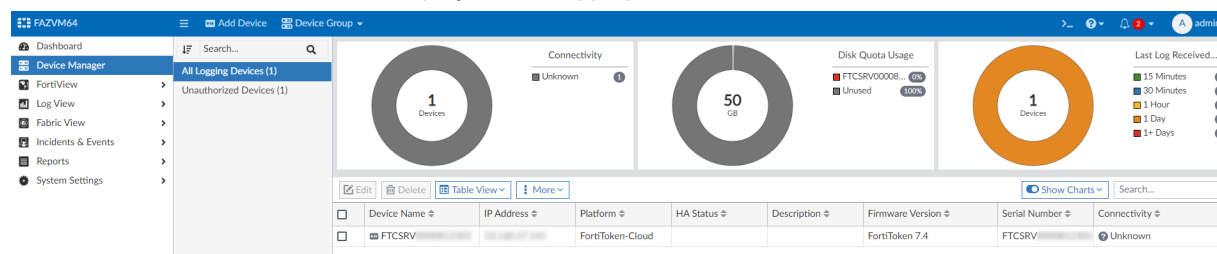
The FortiToken Cloud displays in the *Unauthorized Devices* list.

The screenshot shows the FortiAnalyzer Device Manager page. The left sidebar is the same as the dashboard. The main area displays a table of unauthorized devices with columns: Device Name, Platform, Serial Number, IP Address, Firmware Version, and Management Mode. The table contains one entry: FTCSRVR, FortiToken-Cloud, FTCSRVR, 10.10.10.10, FortiToken 7.4, and Configuration & Logging.

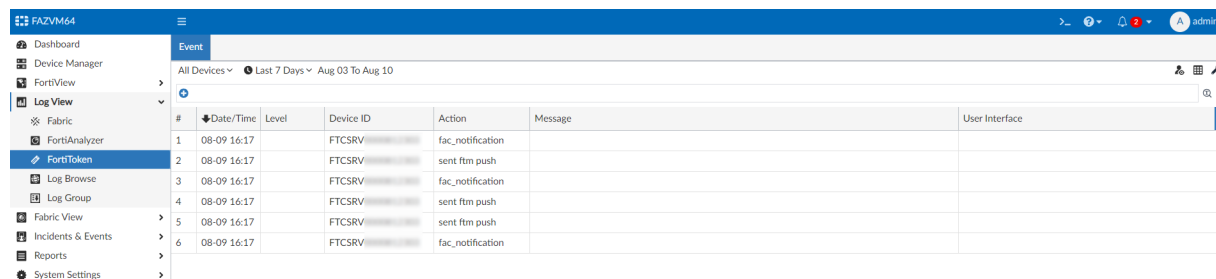
Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
FTCSRVR	FortiToken-Cloud	FTCSRVR	10.10.10.10	FortiToken 7.4	Configuration & Logging

3. Select the FortiToken Cloud device and click *Authorize*.

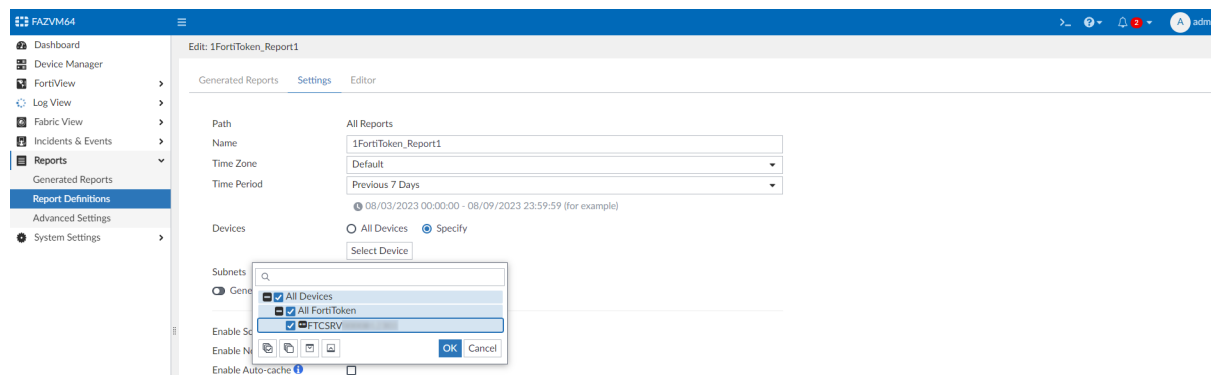
The FortiToken Cloud device now displays in *All Logging Devices* list.



The FortiToken Cloud logs display in *Log View > FortiToken*.



The FortiToken Cloud device can now be used in *Reports*.



## Log Forwarding

This section lists the new features added to FortiAnalyzer for log forwarding:

- [Fluentd support for public cloud integration on page 30](#)

## Fluentd support for public cloud integration

You can create output profiles to configure log forwarding to public cloud services.

### To create an output profile for log forwarding:

1. Go to *System Settings > Advanced > Log Forwarding > Output Profile*.
2. Click *Create New*.

The *Create Output Profile* pane displays.

3. Configure the following options:

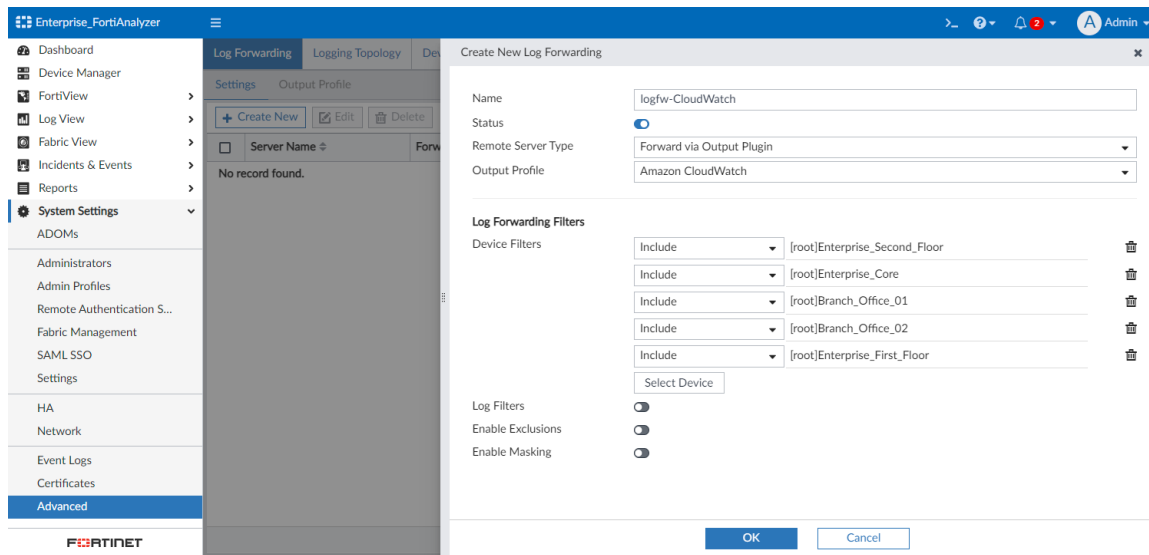
<b>Name</b>	Enter a name for the output profile.
<b>Type</b>	Select the public cloud service for the output profile.
<b>Configuration</b>	<p>Click <i>Use Default</i> to use the default Fluentd configuration for the selected public cloud service.</p> <p>Alternatively, copy and paste the Fluentd configuration into this field for the selected public cloud service.</p>
<b>Field</b>	<p>Fields will automatically be added into the configuration if a keyword matches the placeholder in the configuration to provide encryption for you to hide the credentials.</p> <p>For example, a password placeholder in the configuration would be "\${password}". In the field, you can define <i>Field</i>: password, <i>Value</i>: actual_password.</p>

4. Click *Validate and Save*.

### To configure log forwarding to the output profile:

1. Go to *System Settings > Advanced Log Forwarding > Settings*.
2. Click *Create New*.

The *Create New Log Forwarding* pane displays.



### 3. Configure the following options:

<b>Name</b>	Enter a name for the remote server.
<b>Status</b>	Enable log forwarding.
<b>Remote Server Type</b>	Select <i>Forward via Output Plugin</i> .
<b>Output Profile</b>	Select the output profile.
<b>Log Forwarding Filters</b>	
<b>Device Filters</b>	Click <i>Select Device</i> , then select the devices whose logs will be forwarded.
<b>Log Filters</b>	Enable to configure filters for the logs that are forwarded.
<b>Enable Exclusions</b>	Enable to configure filter on the logs that are forwarded.
<b>Enable Masking</b>	Enable log field masking, if needed.

### 4. Click OK.

To troubleshoot the Fluentd connection with the FortiAnalyzer CLI:

#### 1. In the FortiAnalyzer CLI, enter the following command to check the Fluentd write status:

```
FAZVM64 # diagnose test application fwdpluginind 4
Stats for plugin:
lfw_name: logfw-CloudWatch
plugin_name: Amazon CloudWatch
type: AMAZON_CLOUDWATCH
fd-plugin-id: tcp_1_3da_6af_922_1c3
fluentd emit stats(emit_calls|emit_rec_calls|emit_size): 3685, 88677, 0
fluentd write stats(write|retry|rollback): 3, 0, 0
fluentd buffer queue(byte_size|total_queue_size|queue_len|ratio): 49842536,
52433884, 2, 0
fluentd buffer stage(byte_size|stage_length): 4325288, 1
fluentd flush stats(flush_time|slow_flush_count): 0, 0
```

#### 2. In the FortiAnalyzer CLI, enter the following command to determine if the Fluentd log files are present:

```
FAZVM64 # diagnose sql fluentd log-tail
Fluentd log files are not present. Please turn on Fluentd log first if you need to
test it.
```

**3. In the FortiAnalyzer CLI, enter the following command to enable Fluentd logging:**

```
FAZVM64 # diagnose test application fwdplugind 201 log enable
Warning: This will enable Fluentd logging.
Fluentd requires a restart for changes to take effect. The restart will disrupt
Fluentd's current log handling.
Execute the command again in one minute for the changes to take effect.
FAZVM64 # diagnose test application fwdplugind 201 log enable
Fluentd logging is enabled, Fluentd will be restarted.
```

**4. In the FortiAnalyzer CLI, enter the following command again to show the processed events:**

```
FAZVM64 # diagnose sql fluentd log-tail
File /drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log, is present, will
open it.
Please press Control+C to exit.
=====
aws_sec_key xxxxxx
region "us-west-2"
log_group_name "Log-Group-Test"
log_stream_name "Log-Stream-test"
auto_create_stream true
@id tcp_1_3da_6af_922_1c3
<buffer tag,time>
@type "memory"
chunk_limit_size 10M
total_limit_size 50M
timekey 5m
timekey_wait 30s
timekey_use_utc true
flush_thread_count 3
flush_at_shutdown true
overflow_action block
retry_forever true
disable_chunk_backup true
</buffer>
</match>
</worker>
</ROOT>
2023-04-24 16:05:20 -0700 [info]: starting fluentd-1.15.2 pid=12376 ruby="2.7.6"
2023-04-24 16:05:20 -0700 [info]: spawn command to main: cmdline=
["/usr/local/fluentd/td-agent/bin/ruby", "-Eascii-8bit:ascii-8bit",
"/usr/sbin/td-agent", "-d", "/drive0/private/fwdplugind/fluentd/faz-td-
agent.pid", "-c", "/drive0/private/fwdplugind/fluentd/faz-td-agent.conf", "-
o", "/drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log", "--log-rotate-
size", "5120000", "--under-supervisor"]
2023-04-24 16:05:20 -0700 [info]: #0 adding match pattern="tcp_1" type="cloudwatch_
logs"
2023-04-24 16:05:21 -0700 [info]: adding source type="monitor_agent"
2023-04-24 16:05:21 -0700 [info]: #0 adding source type="tcp"
2023-04-24 16:05:21 -0700 [info]: #0 starting fluentd worker pid=12390 ppid=12387
worker=0
2023-04-24 16:05:21 -0700 [info]: #0 listening tcp socket bind="127.0.0.1"
port=10000
2023-04-24 16:05:21 -0700 [info]: #0 fluentd worker is now running worker=0
```

## Reports

This section lists the new features added to FortiAnalyzer for reports:

- [Report guidance on page 34](#)
- [PCI Security Rating Report on page 36](#)
- [Cyber Threats Assessment Report update on page 37](#)
- [Threat Report update on page 38](#)
- [FSBP Security Rating Report on page 40](#)
- [CIS Controls Security Rating report on page 41](#)
- [Shadow IT Report on page 42](#)
- [FortiADC Report 7.4.1 on page 43](#)
- [Default ZTNA Report 7.4.1 on page 45](#)

## Report guidance



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [Report guidance](#)

---

FortiAnalyzer provides many factory default reports that use charts relying on specific log types and log fields to provide valuable output. When running a full report, you may see "No Data" returned in sections if:

- logging was not enabled correctly
- the report element is for a different Device/Log Type
- there are no matching logs

Debugging such scenarios can be time consuming because it requires navigating through charts, macros, and datasets.

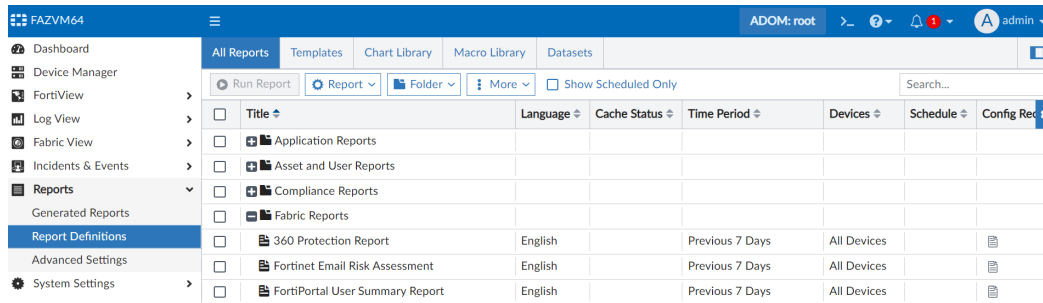
To improve the overall reporting experience, a new *Report Guidance* feature has been implemented to provide full visibility for each report element in terms of:

- Device Type (e.g. Fortigate)
- Log Type (e.g. traffic)
- Log Fields (e.g. action, itime)

In short, you can use the *Report Guidance* feature to troubleshoot and determine if FortiAnalyzer has the appropriate Analytics logs available for a report.

### To use the Report Guidance feature:

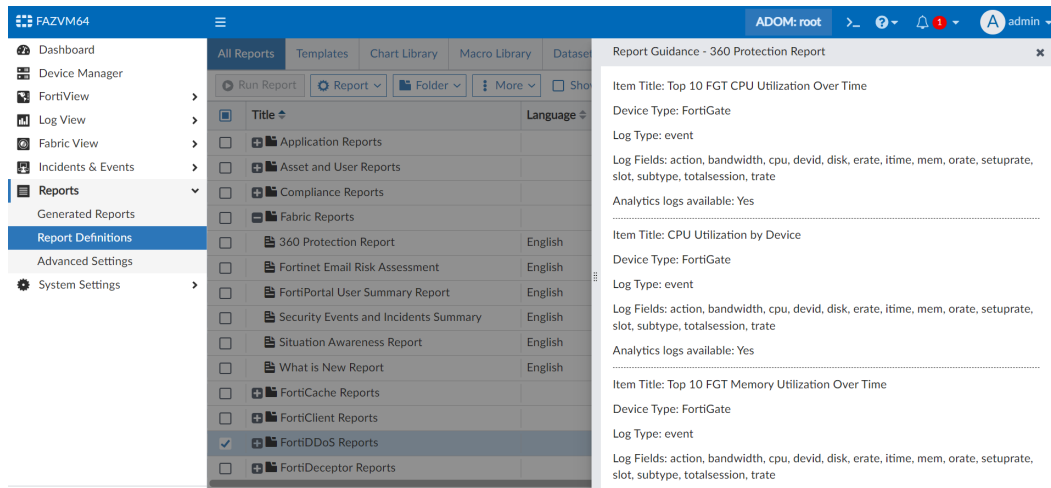
1. Go to *Reports > Report Definitions > All Reports*.  
There is a new *Config Recommendation* column.



Title	Language	Cache Status	Time Period	Devices	Schedule	Config Recommendation
Application Reports						
Asset and User Reports						
Compliance Reports						
Fabric Reports						
360 Protection Report	English		Previous 7 Days	All Devices		
Fortinet Email Risk Assessment	English		Previous 7 Days	All Devices		
FortiPortal User Summary Report	English		Previous 7 Days	All Devices		

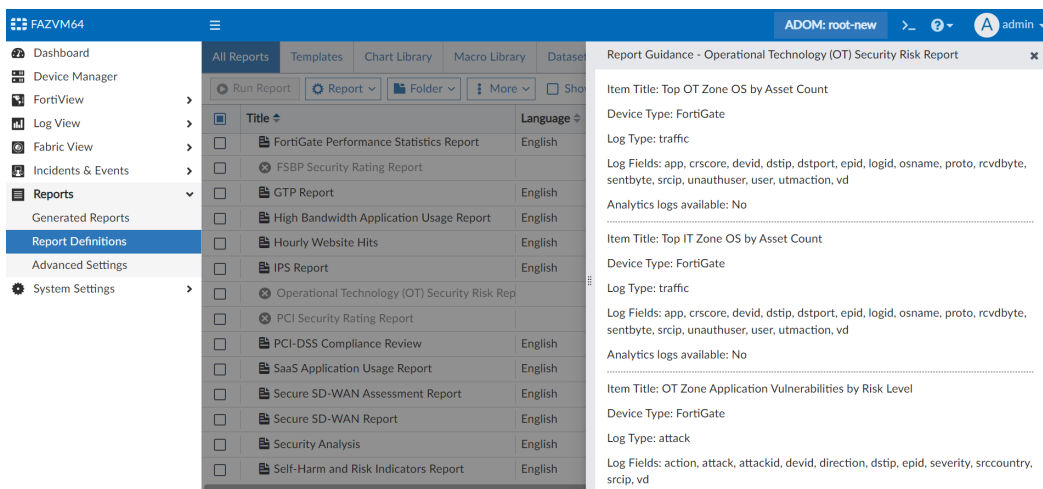
2. Click the icon in the *Config Recommendation* column.

The *Report Guidance* pane opens for that report. This pane provides the *Item Title* (chart or macro name), *Device Type*, *Log Type*, and the relevant *Log Fields* and *Analytics log availability*.



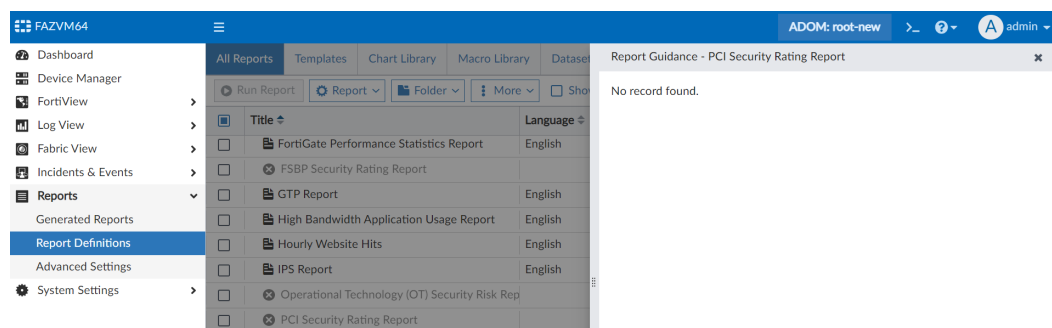
Item Title	Device Type	Log Type	Log Fields	Analytics logs available
Top 10 FGT CPU Utilization Over Time	FortiGate	event	action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate	Yes
CPU Utilization by Device	FortiGate	event	action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate	Yes
Top 10 FGT Memory Utilization Over Time	FortiGate	event	action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate	Yes

The *Report Guidance* pane is available for license-controlled reports, but the report cannot be generated without a valid license.



Item Title	Device Type	Log Type	Log Fields	Analytics logs available
Top OT Zone OS by Asset Count	FortiGate	traffic	app, crscore, devid, dstip, dstport, epid, logid, osname, proto, rcvdbyte, sentbyte, srcip, unauthuser, user, utmaction, vd	No
Top IT Zone OS by Asset Count	FortiGate	traffic	app, crscore, devid, dstip, dstport, epid, logid, osname, proto, rcvdbyte, sentbyte, srcip, unauthuser, user, utmaction, vd	No
OT Zone Application Vulnerabilities by Risk Level	FortiGate	attack	action, attack, attackid, devid, direction, dstip, epid, severity, srccountry, srcip, vd	No

For reports that are not generated with log tables, such as the FSBP/PCI or CIS Security Rating Reports, the *Report Guidance* pane will indicate *No record found*.

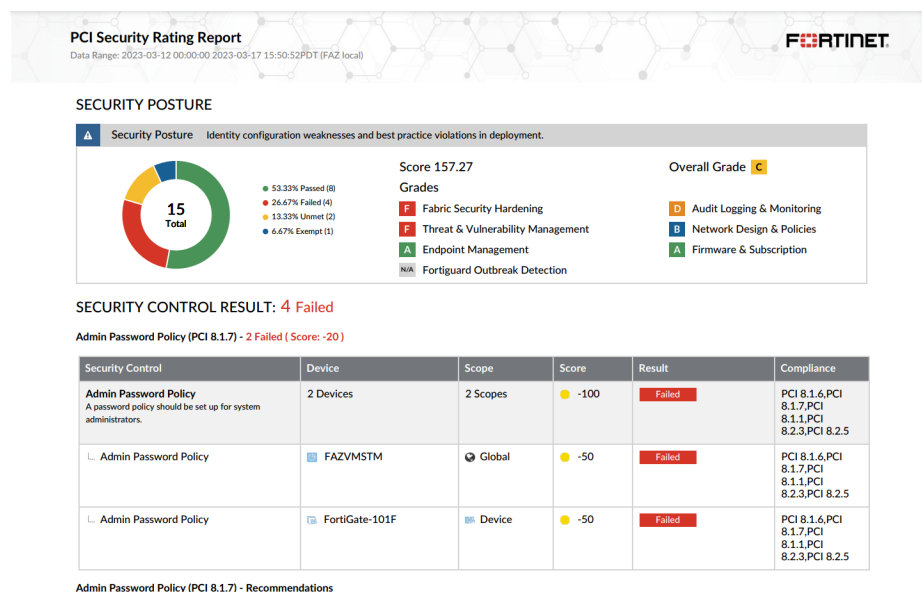


## PCI Security Rating Report

A *PCI Security Rating Report* is now available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization* based on PCI DSS 3.2 standards. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

For example, see a sample of page 1 from the report in PDF format below.

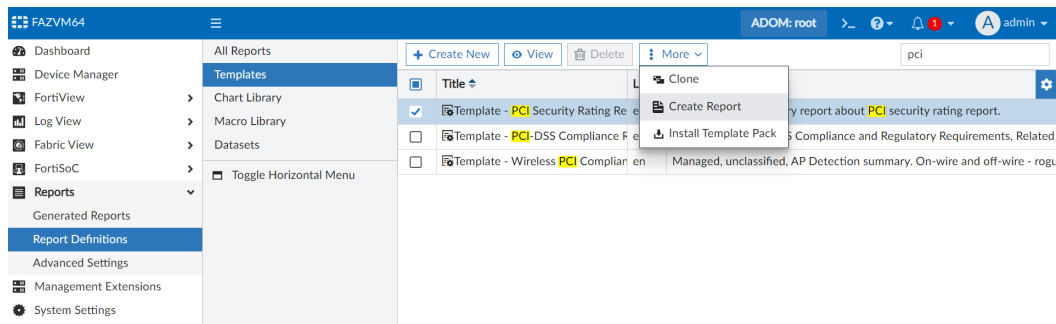


Admin Password Policy (PCI 8.1.7) - Recommendations

### To create the report from the template:

- Go to **Reports > Report Definitions > Templates**.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
- Select the checkbox for *Template - PCI Security Rating Report*.
- From the *More* dropdown, click *Create Report* to create a report using the template.  
You can also click *Clone* to clone the template and make adjustments.





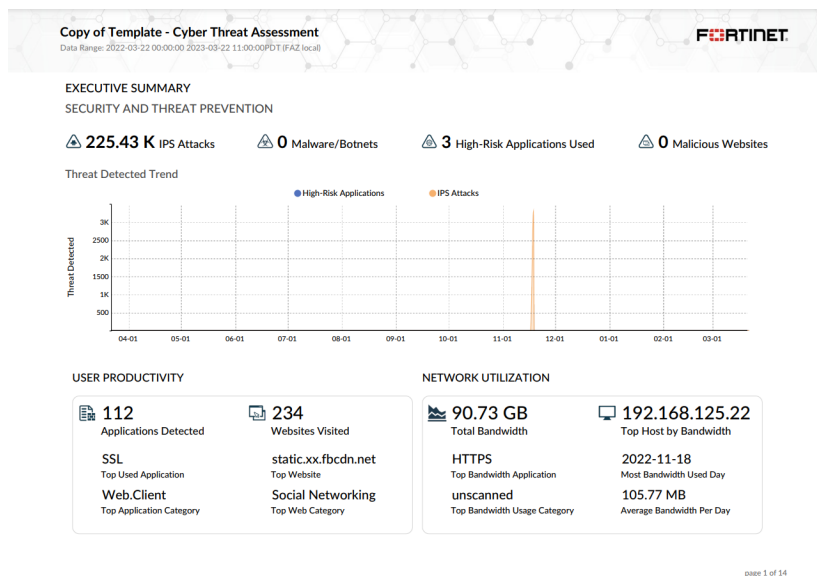
### To run the PCI Security Rating Report:

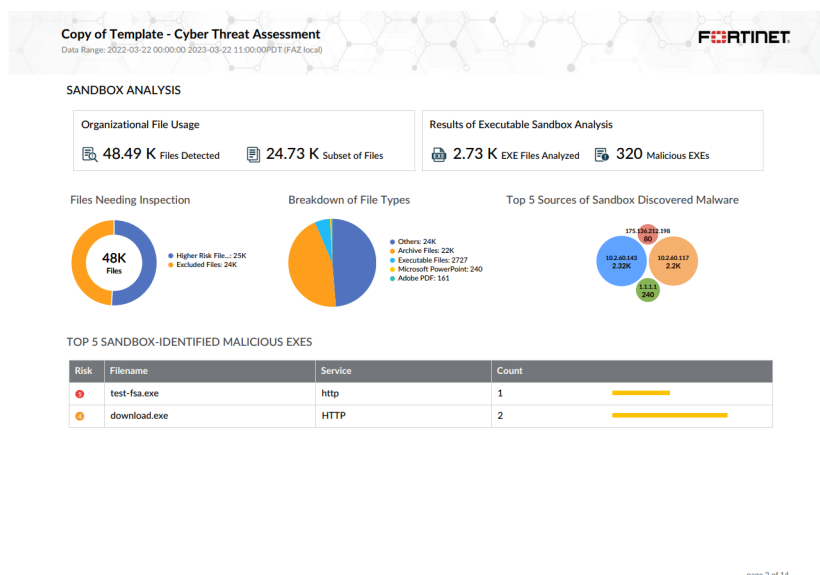
1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *PCI Security Rating Report*. The *Edit: PCI Security Rating Report* pane opens.
2. Click *Run Report*.  
Once the report is available, click the format to view the report in.

## Cyber Threats Assessment Report update

The existing *Cyber Threats Assessment Report* has been updated with new style and content to enhance the visibility of the provided data.

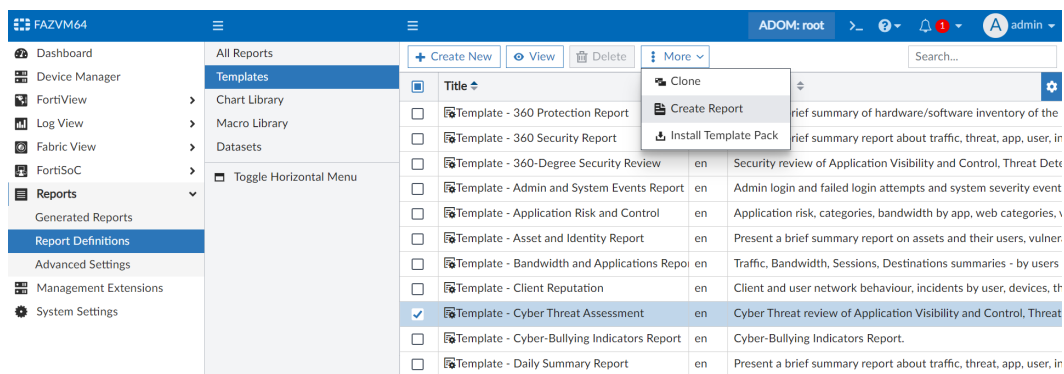
For example, see a sample of the report in PDF format below:





### To create the report from the template:

- Go to **Reports > Report Definitions > Templates**.  
From the *Preview* column, you can click **PDF** or **HTML** to preview the report in that format.
- Select the checkbox for **Template - Cyber Threats Assessment Report**.
- From the **More** dropdown, click **Create Report** to create a report using the template.  
You can also click **Clone** to clone the template and make adjustments.



### To run the Cyber Threats Assessment Report:

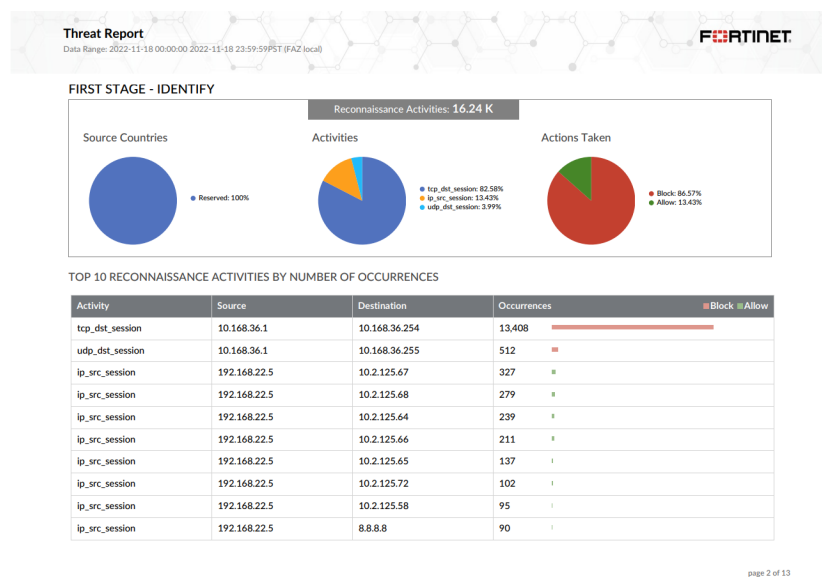
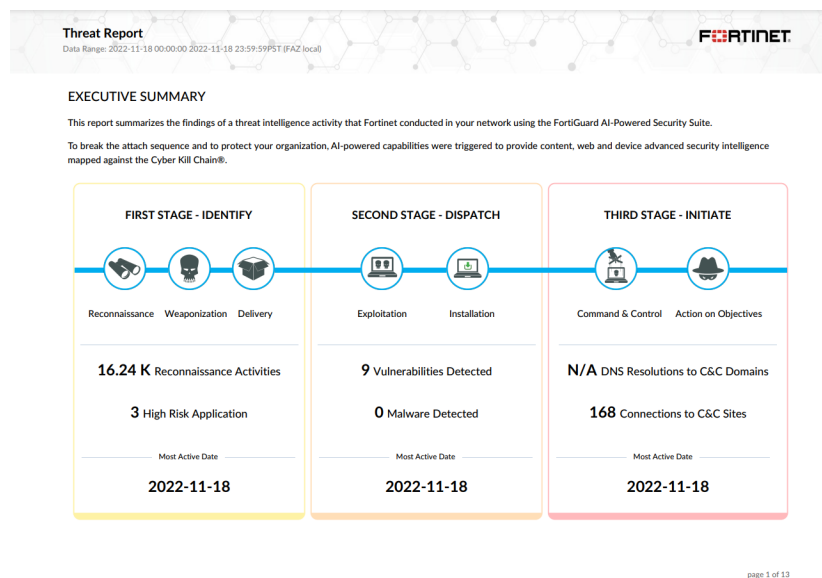
- Go to **Reports > Report Definitions > All Reports**, and double-click the row for the **Cyber Threats Assessment Report**.  
The **Edit: Cyber Threats Assessment Report** pane opens.
- Click **Run Report**.  
Once the report is available, click the format to view the report in.

## Threat Report update

The **Threat Report** has been updated to provide the following:

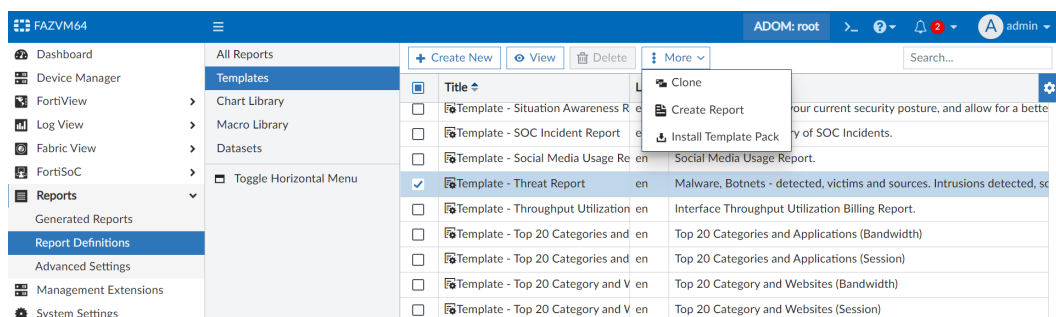
- New style and content to better present threat data
- Threats are mapped to the Cyber Kill Chain stages for correlation and pattern identification

For example, see a sample of the report in PDF format below:



### To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Threat Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.  
You can also click *Clone* to clone the template and make adjustments.



### To run the Threat Report:

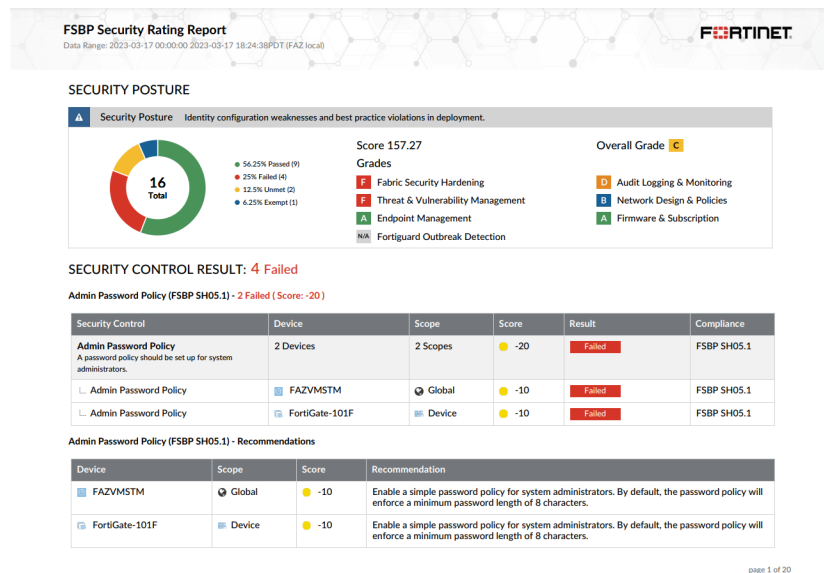
1. Go to **Reports > Report Definitions > All Reports**, and double-click the row for the **Threat Report**. The **Edit: Threat Report** pane opens.
2. Click **Run Report**.  
Once the report is available, click the format to view the report in.

## FSBP Security Rating Report

A FSBP (Fortinet Security Best Practices) Security Rating Report is available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization*. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

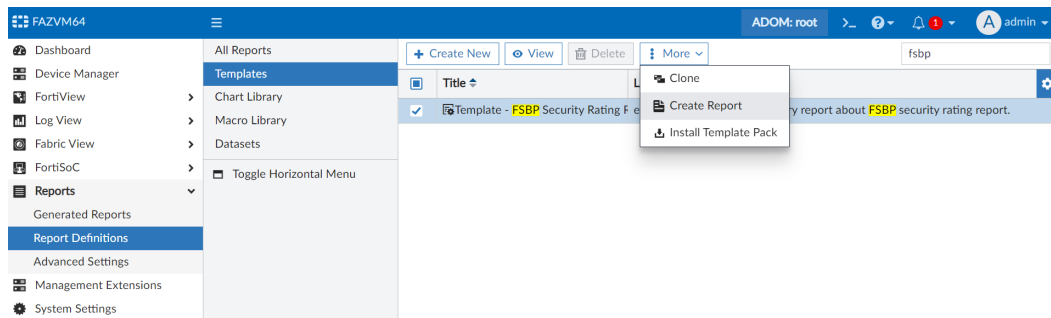
For example, see a sample of page 1 from the report in PDF format below.



### To create the report from the template:

1. Go to **Reports > Report Definitions > Templates**.  
From the **Preview** column, you can click **PDF** or **HTML** to preview the report in that format.

2. Select the checkbox for *Template - FSBP Security Rating Report*.
  3. From the *More* dropdown, click *Create Report* to create a report using the template.
- You can also click *Clone* to clone the template and make adjustments.

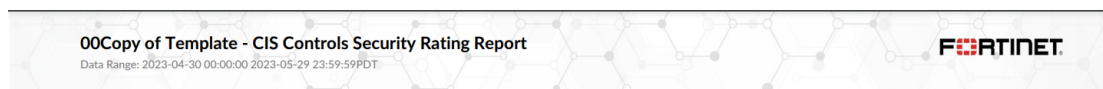


### To run the FSBP Security Rating Report:

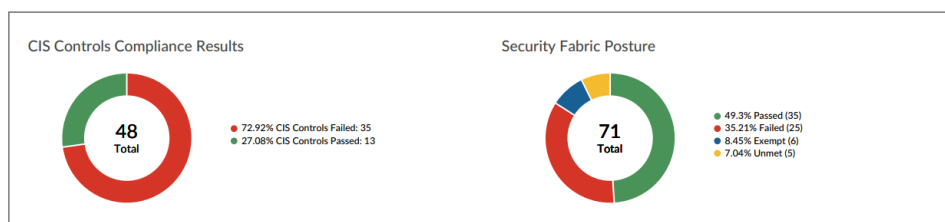
1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *FSBP Security Rating Report*. The *Edit: FSBP Security Rating Report* pane opens.
  2. Click *Run Report*.
- Once the report is available, click the format to view the report in.

## CIS Controls Security Rating report

A *CIS Controls Security Rating Report* is now available on FortiAnalyzer. This report includes CIS mapping information. For example, see a sample of the report in PDF format below.



### EXECUTIVE SUMMARY



### OVER VIEW

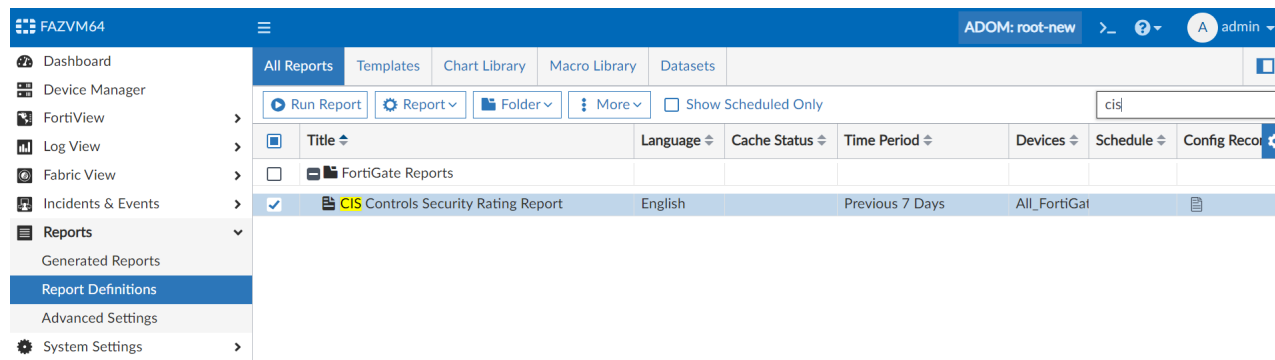
#### CIS CRITICAL SECURITY CONTROL

CIS Control	CIS Name	Failed, Unmet or Exempt (# of Devices)	Passed (# of Devices)
<b>CIS Control 1</b>	<b>Inventory and Control of Enterprise Assets</b>	1	0
└ CIS Control 1.1	Establish and Maintain Detailed Enterprise Asset Inventory	1	0
└ CIS Control 1.2	Address Unauthorized Assets	0	0
<b>CIS Control 3</b>	<b>Data Protection</b>	1	0
└ CIS Control 3.3	Configure Data Access Control Lists	1	0
└ CIS Control 3.10	Encrypt Sensitive Data in Transit	1	0
└ CIS Control 3.12	Segment Data Processing and Storage Based on Sensitivity	1	0

page 1 of 19

### To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - CIS Controls Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.  
You can also click *Clone* to clone the template and make adjustments.



### To run the CIS Controls Security Rating Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *CIS Controls Security Rating Report*.  
The *Edit: CIS Controls Security Rating Report* pane opens.
2. Click *Run Report*.  
Once the report is available, click the format to view the report in.

## Shadow IT Report

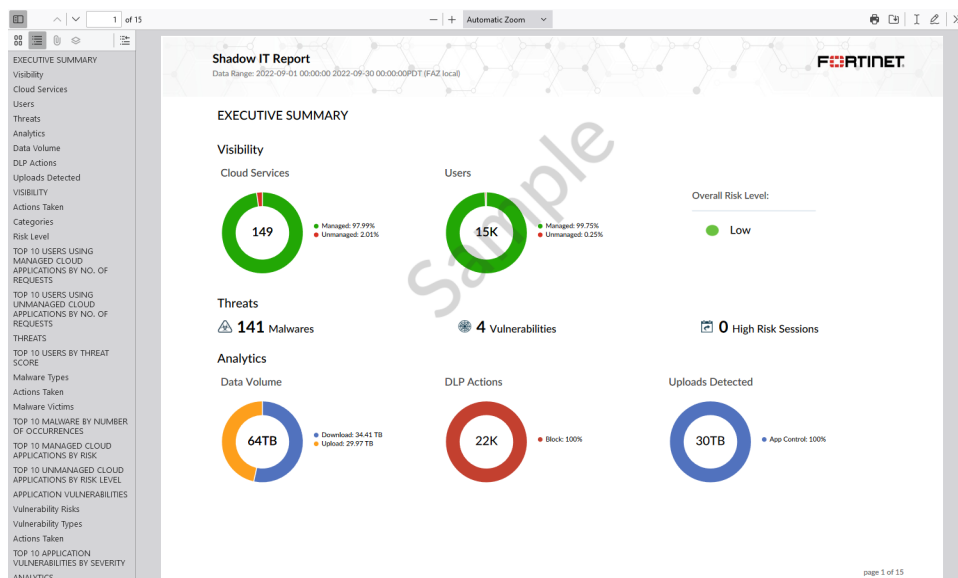
The *Shadow IT Report* is now available on FortiAnalyzer.

This report provides enhanced visibility and control for cloud based applications.

Detected applications are classified as:

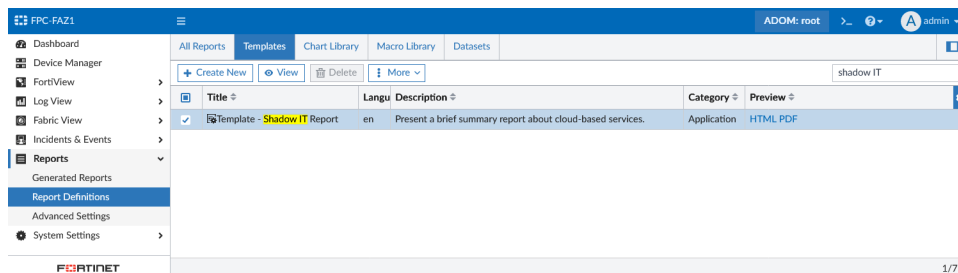
- Managed > Allowed
- Unmanaged > Blocked/Quarantined/Reset

For example, see a sample of page 1 from the report in PDF format below.



### To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Shadow IT Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.  
You can also click *Clone* to clone the template and make adjustments.



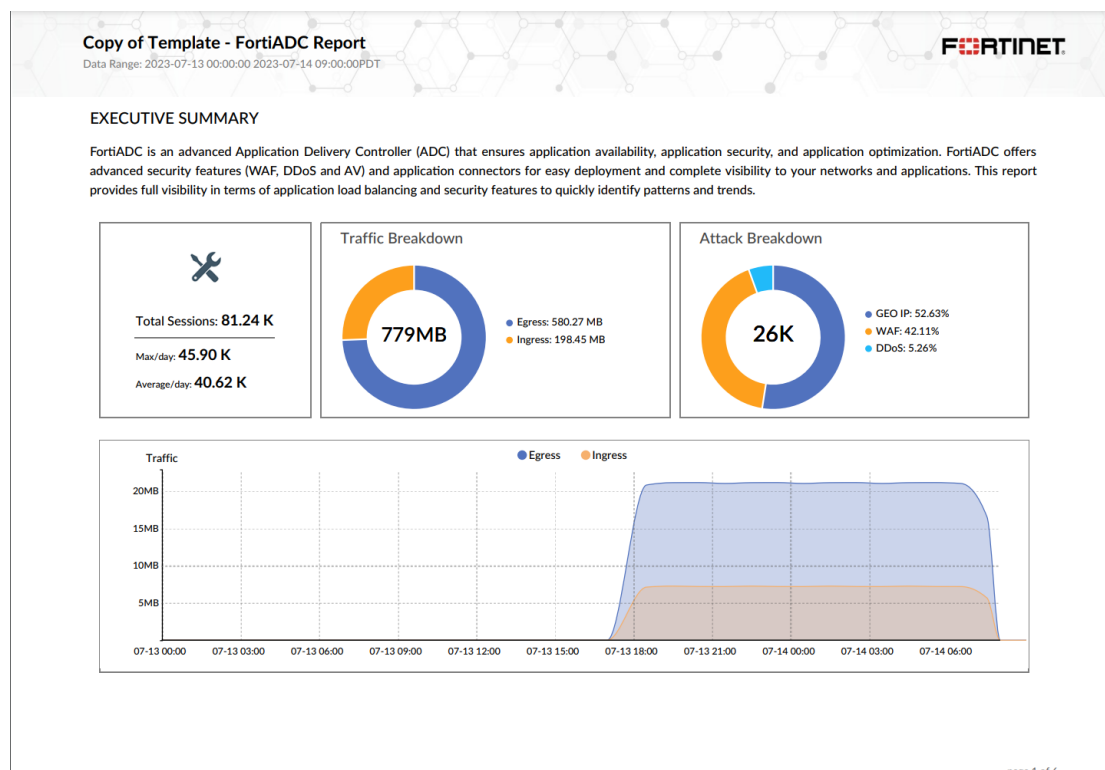
### To run the Shadow IT Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *Shadow IT Report*.  
The *Edit: Shadow IT Report* pane opens.
2. Click *Run Report*.  
Once the report is available, click the format to view the report in.

## FortiADC Report - 7.4.1

The *FortiADC Report* is available on FortiAnalyzer to offer comprehensive visibility into application load balancing and security features, enabling rapid identification of security patterns and trends associated with the use of the product.

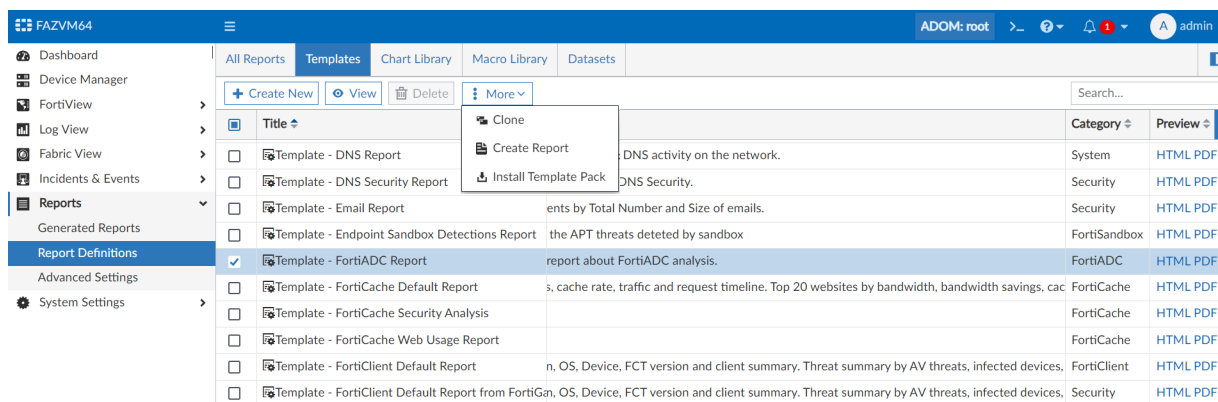
For example, see a sample of page 1 from the report in PDF format below.



This report requires that a FortiADC device has been added and authorized to the FortiAnalyzer.

### To create the report from the template:

- Go to **Reports > Report Definitions > Templates**.  
From the *Preview* column, you can click **PDF** or **HTML** to preview the report in that format.
- Select the checkbox for **Template - FortiADC Report**.
- From the **More** dropdown, click **Create Report** to create a report using the template.  
You can also click **Clone** to clone the template and make adjustments.



### To run the FortiADC Report:

- Go to **Reports > Report Definitions > All Reports**, and double-click the row for the **FortiADC Report**.  
The **Edit: FortiADC Report** pane opens.



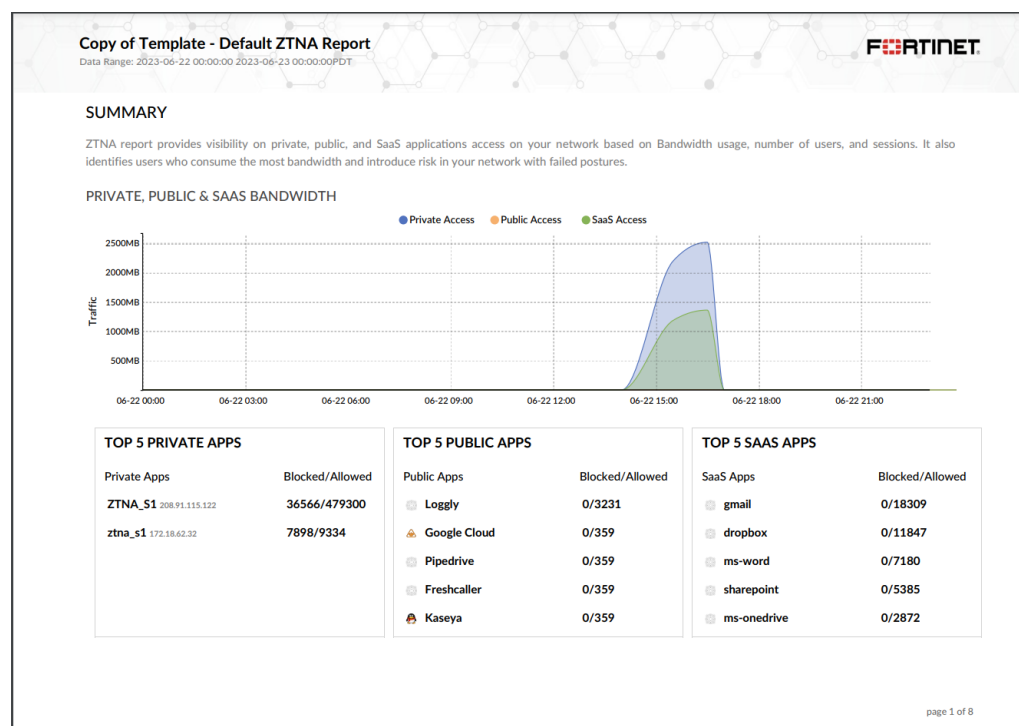
## 2. Click *Run Report*.

Once the report is available, click the format to view the report in.

## Default ZTNA Report - 7.4.1

The *Default ZTNA Report* is now available on FortiAnalyzer to enhance visibility in terms of applications being used with the corresponding bandwidth used and sessions. To better differentiate accessibility and deployments, applications are grouped as private, public, and SaaS. Users that present security risks due to failing security postures can be quickly identified.

For example, see a sample of page 1 from the report in PDF format below.



### To create the report from the template:

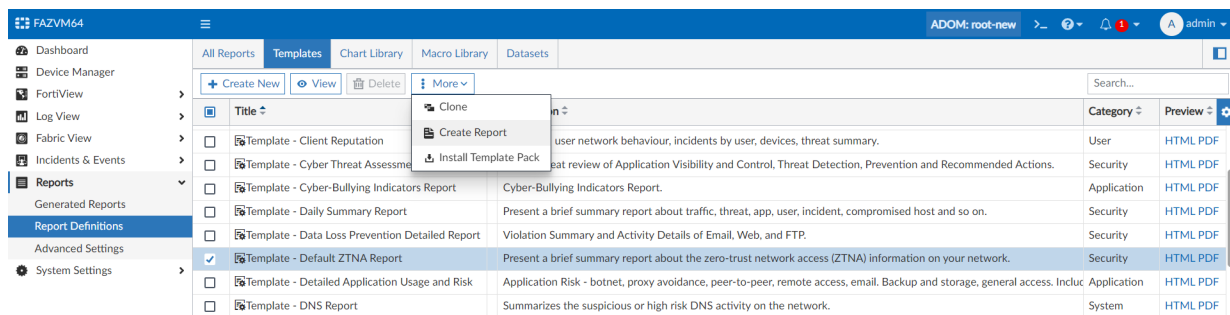
#### 1. Go to *Reports > Report Definitions > Templates*.

From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.

#### 2. Select the checkbox for *Template - Default ZTNA Report*.

#### 3. From the *More* dropdown, click *Create Report* to create a report using the template.

You can also click *Clone* to clone the template and make adjustments.



### To run the Default ZTNA Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *Default ZTNA Report*. The *Edit: Default ZTNA Report* pane opens.
2. Click *Run Report*.  
Once the report is available, click the format to view the report in.

## Others

This section lists the new features added to FortiAnalyzer for other topics relating to logging and reporting:

- [Time zone settings per ADOMs/Reports on page 46](#)

## Time zone settings per ADOMs/Reports



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [Creating ADOMs](#)
- [Report Settings tab](#)

To allow a more granular reporting experience for Global deployment, different timezones can be configured on each ADOM/Report.

The *Default* time zone used for this setting is the time zone set for the FortiAnalyzer.

### To configure the time zone for an ADOM:

1. Go to *System Settings > ADOMs*.
2. Edit or create a new ADOM.
3. From the *Time Zone* dropdown, select a time zone for the ADOM.

This time zone will be used when displaying data in *Log View* and *FortiView* for this ADOM.

4. Click OK to save.

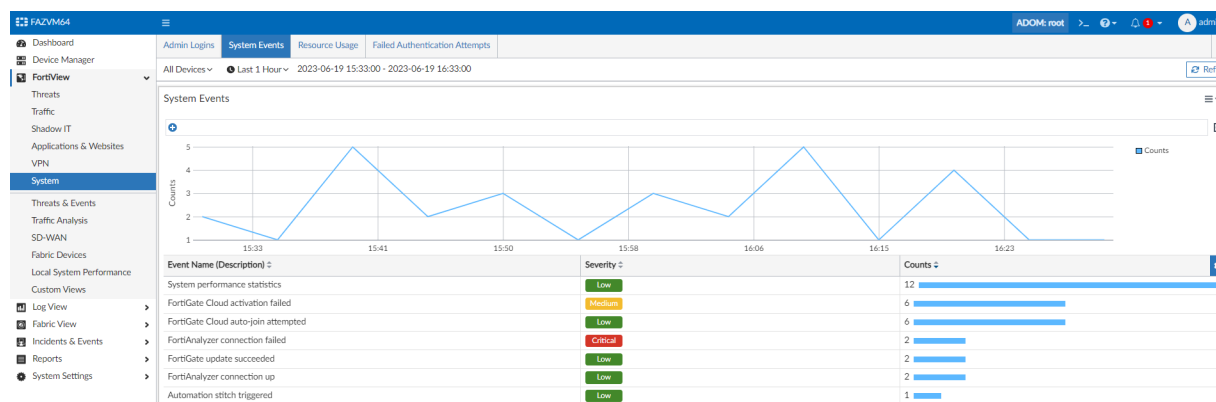
### Example:

In this example, the system time zone is (GMT-8:00) Pacific Time, which is used by the root ADOM. The admin creates a new adom (ADOM1) and sets the time zone to (GMT-5:00) Eastern Time:

In the root ADOM, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according to the default system time zone: (GMT-8:00) Pacific Time.

For example, the admin is reviewing the panes below at approximately 16:30 Pacific Time.

#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	16:30:02	FG800D3915800X	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.7 KB	
2	16:29:57	FG800D3915800X	✓accept	127.0.0.1		127.0.0.1	udp/12121	udp/12121	3.6 KB/0.0 KB	
3	16:29:42	FG800D3915800X	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.1 KB	
4	16:29:42	FG800D3915800X	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.7 KB	
5	16:29:17	FG800D3915800X	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/7.5 KB	
6	16:29:17	FG800D3915800X	✓accept	192.168.1.1		208.91.112.61	NTP	NTP	76.0 B/76.0 B	
7	16:29:17	FG800D3915800X	✓accept	192.168.1.1		208.91.112.63	NTP	NTP	76.0 B/76.0 B	
8	16:29:12	FG800D3915800X	✓accept	192.168.1.1		208.91.112.60	NTP	NTP	76.0 B/76.0 B	
9	16:28:37	FG800D3915800X	✓accept	192.168.1.1		208.91.112.62	NTP	NTP	76.0 B/76.0 B	
10	16:27:52	FG800D3915800X	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.7 KB/7.5 KB	

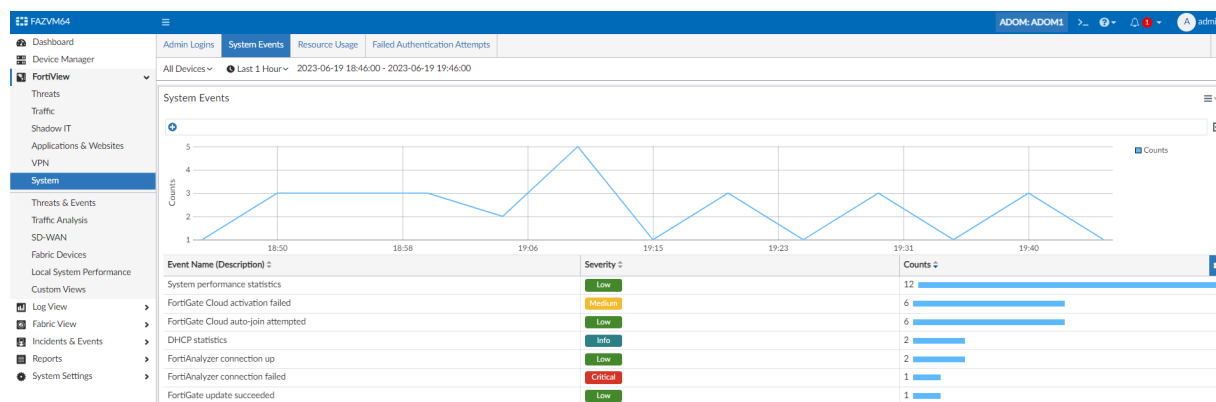


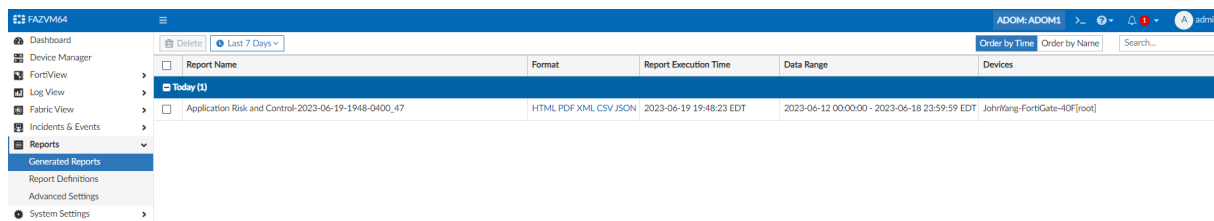
In ADOM1, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according to the ADOM's specified time zone: (GMT-5:00) Eastern Time.

For example, the admin is reviewing the panes below at approximately 16:40 Pacific Time (19:40 Eastern Time).

The screenshot shows the ADOM1 FortiAnalyzer interface. The left sidebar contains the navigation menu with options like Dashboard, Device Manager, FortiView, and System. The main area is divided into three panes: Log View, FortiView, and Generated Reports. The Log View pane displays a table of log entries, including details like Date/Time, Device ID, Action, Source, User, Destination IP, Service, Application, Sent/Received, and Security Event List.

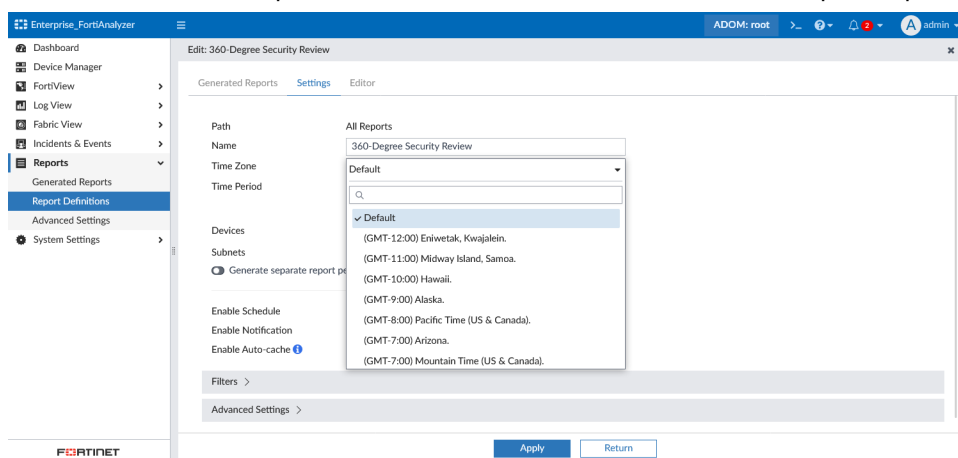
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	19:45:29	FGT40FTK200254	✓close	127.0.0.1		127.0.0.1	HTTP	HTTP	399.0 B/670...	
2	19:44:38	FGT40FTK200254	server-nt	172.16.81.155		173.243.132.25	HTTPS	HTTPS	5.3 KB/8.6 KB	
3	19:43:28	FGT40FTK200254	✓accept	127.0.0.1		127.0.0.1	udp/12121	udp/12121	609.0 B/0.0...	
4	19:43:13	FGT40FTK200254	✓accept	172.16.81.155		208.91.112.62	NTP	NTP	76.0 B/76.0 B	
5	19:42:53	FGT40FTK200254	✓accept	172.16.81.155		208.91.112.60	NTP	NTP	76.0 B/0.0 KB	
6	19:41:13	FGT40FTK200254	✓accept	172.16.81.155		96.45.45.45	DNS	DNS	2.9 KB/26.7...	
7	19:41:08	FGT40FTK200254	✓accept	172.16.81.155		208.91.112.63	NTP	NTP	76.0 B/0.0 KB	
8	19:41:08	FGT40FTK200254	✓accept	172.16.81.155		96.45.46.46	DNS	DNS	3.5 KB/31.0...	
9	19:40:38	FGT40FTK200254	server-nt	172.16.81.155		173.243.143.6	HTTPS	HTTPS	5.4 KB/8.4 KB	
10	19:40:28	FGT40FTK200254	✓close	127.0.0.1		127.0.0.1	HTTP	HTTP	399.0 B/670...	





### To configure the time zone for a report:

1. Go to *Reports > Report Definitions > All Reports*.
2. Double-click the report, or right-click the report and select *Edit*.
3. Go to the *Settings* tab.
4. From the *Time Zone* dropdown, select a time zone to use for data in the report output.



5. Click *Apply* to save.

# System

This section lists the new features added to FortiAnalyzer for system settings:

- [Others on page 50](#)

## Others

This section lists the new features added to FortiAnalyzer for other features relating to system settings:

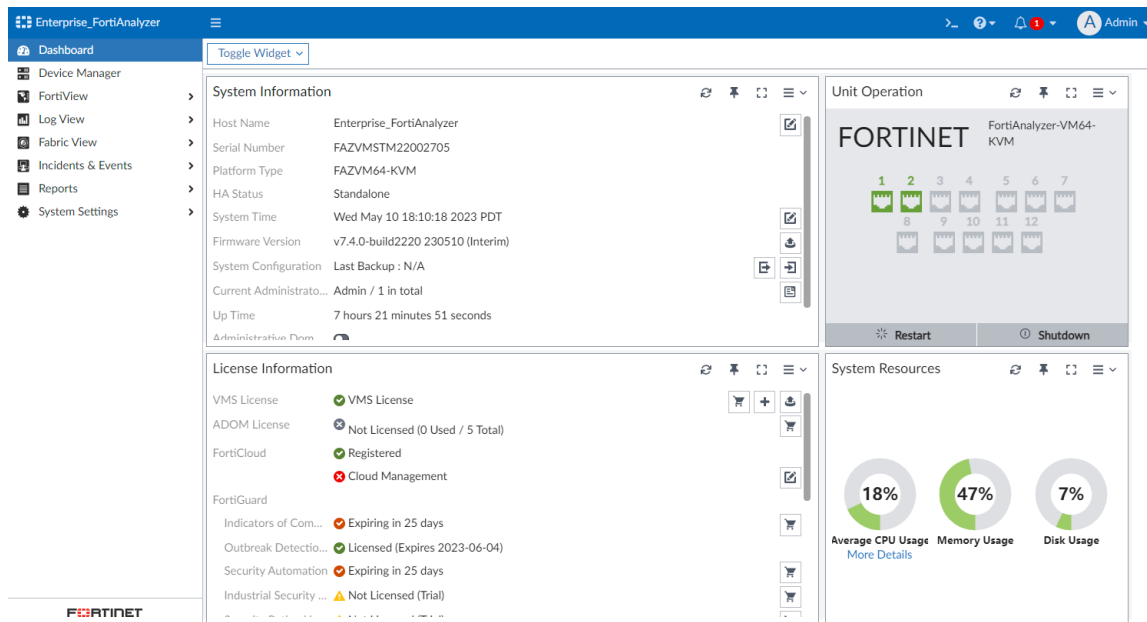
- [FortiAnalyzer GUI enhancements on page 50](#)
- [Fabric of FAZ topology chart on page 54](#)
- [Fabric of FAZ: member authorization with supervisor on page 56](#)
- [Fabric of FAZ global FortiView support on page 61](#)
- [Fabric of FAZ: Central report support and creating Fabric groups on page 63](#)
- [Block out contract device from upgrading to next or major or minor release on page 66](#)

## FortiAnalyzer GUI enhancements

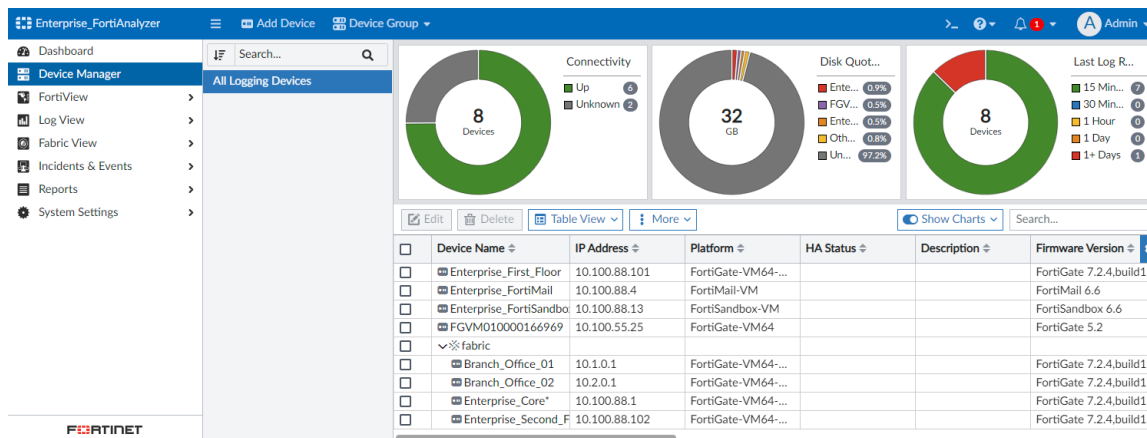
To enhance the user experience and to align to FortiOS, the following changes have been added to the FortiAnalyzer GUI:

- Uses a new and customizable landing page (*Dashboard*)
- Uses Neutrino framework
- Adopts a 3-layer navigation, making all menus accessible via a single click

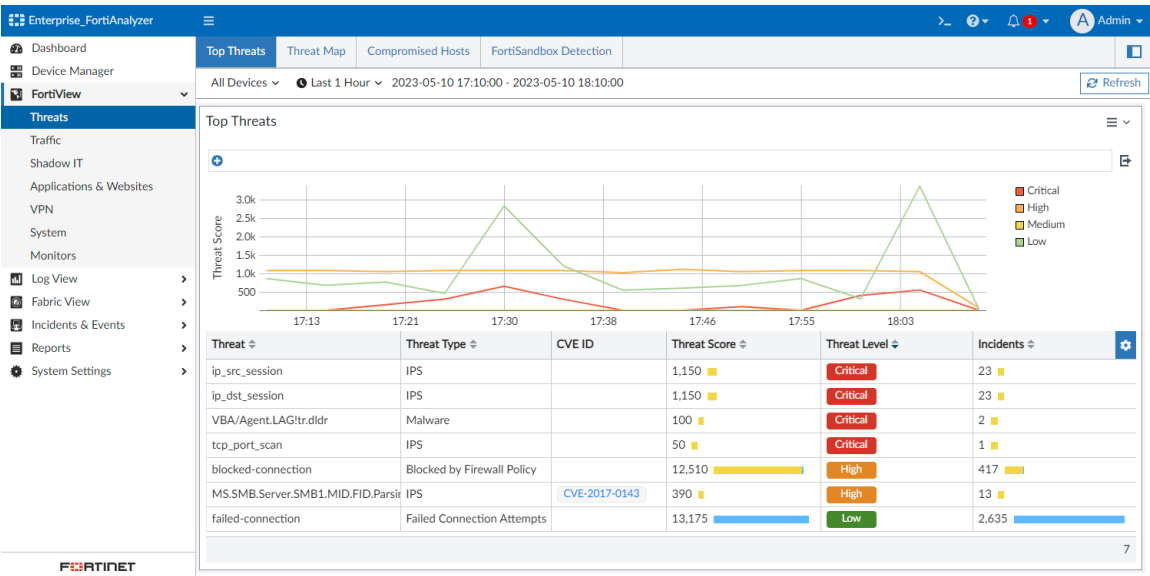
The *Dashboard* includes widgets, such as *Log Status* and *Alert Message Console*. You can toggle which widgets display from the *Toggle Widget* dropdown.



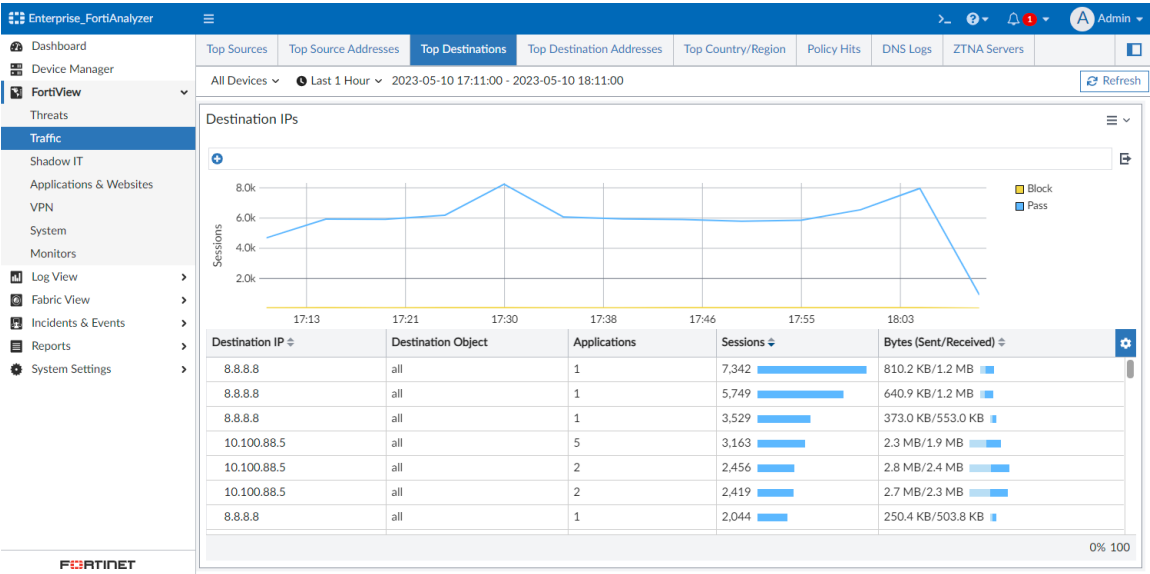
You can access other pages, such as *Device Manager*, from the left-pane navigation.



If there are sub-menus, as in *FortiView*, the left-pane navigation will expand to show other pages in that section.

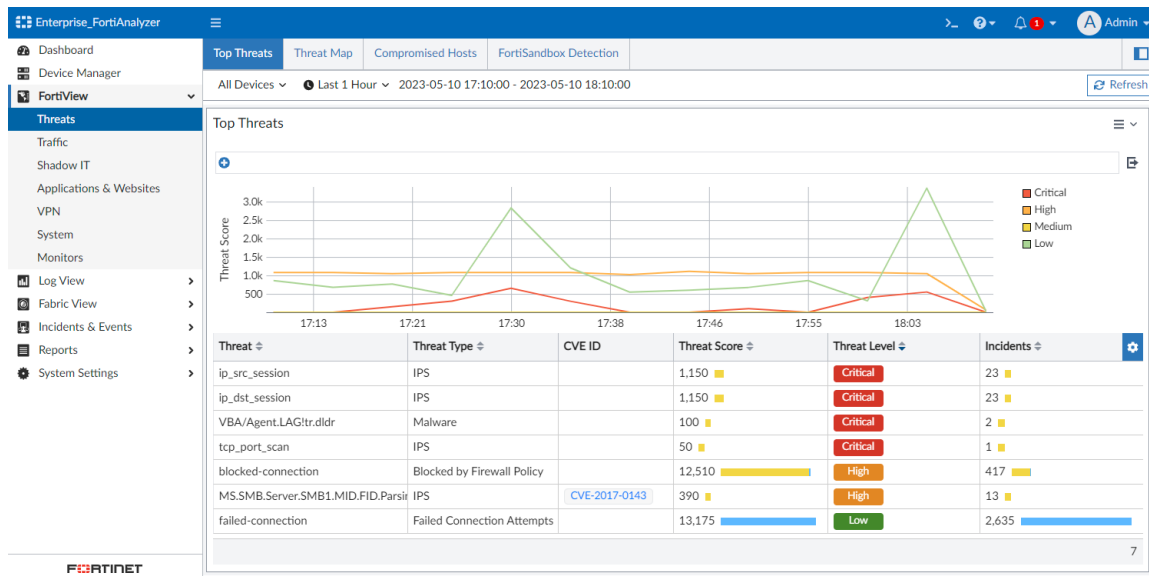


Further sub-menus may also be available along the top of the pane. For example, in the image below, the admin has navigated to *FortiView > Traffic > Top Destinations*.

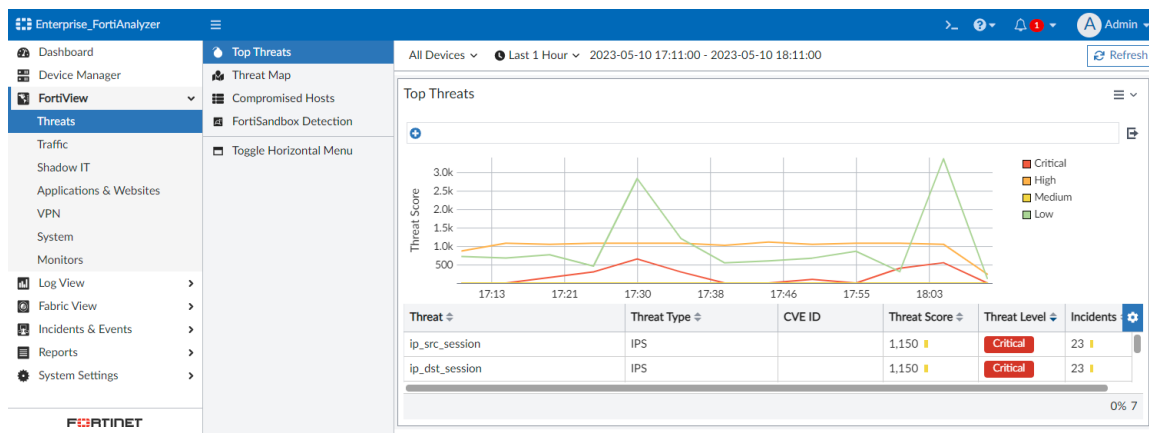


When available, you can click the horizontal view icon (⌵) to switch to a vertical display of the sub-menu. The sub-menu will then display in a left-pane navigation instead.

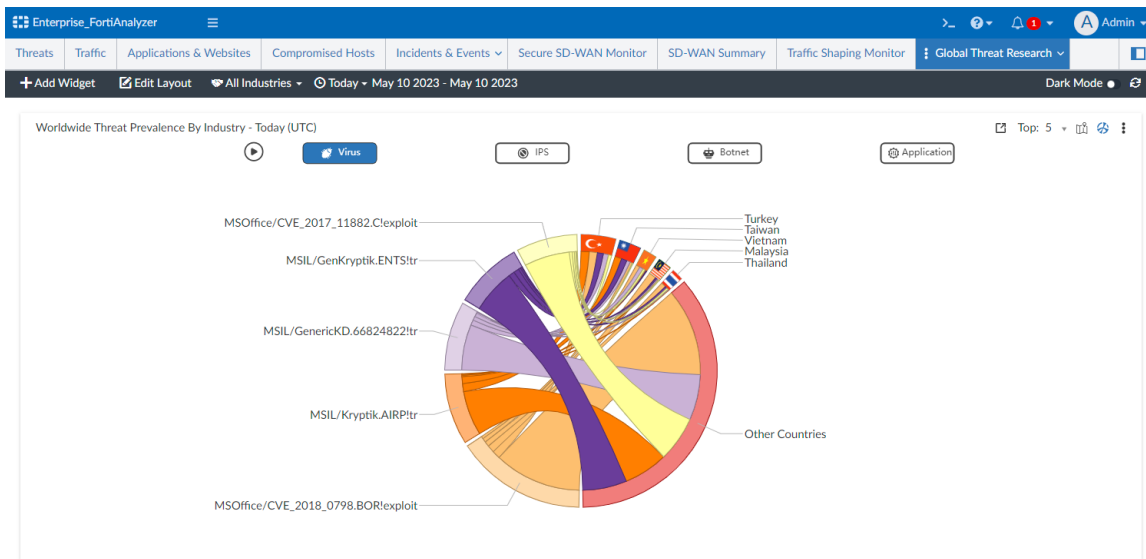




Click **Toggle Horizontal Menu** to return to the horizontal display at the top of the pane.



On any page in the GUI, you can click the menu icon (☰) to hide the left-pane navigation. Click the menu icon (☰) again to re-open the left-pane navigation.



## Fabric of FAZ topology chart



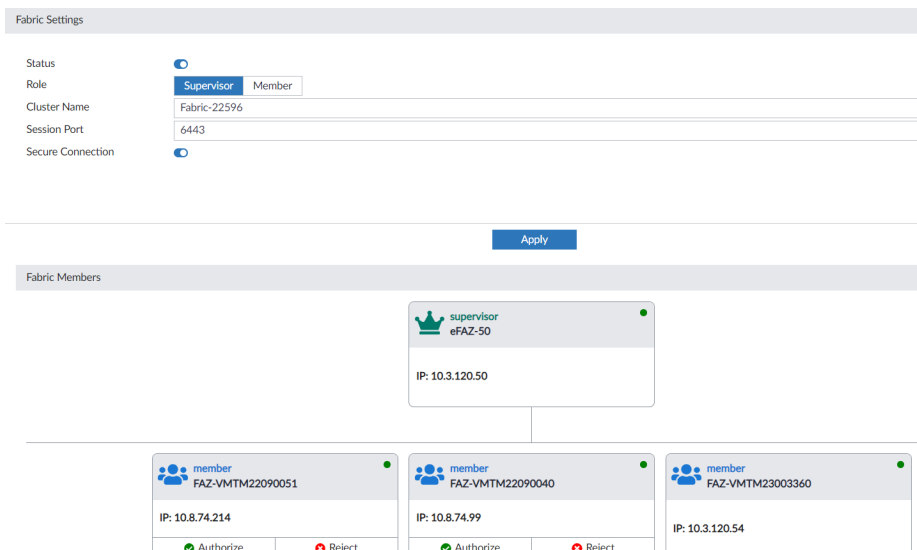
This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- [Configuring the FortiAnalyzer Fabric](#)

A FortiAnalyzer Fabric topology chart is displayed on the supervisor to quickly identify connected members and their corresponding status.

### FortiAnalyzer Fabric supervisor:

To view the topology on the supervisor, go to *System Settings > Fabric Management > Fabric Settings*. In the *Fabric Members* section, the topology displays all connected members.



You can hover over the role for a FortiAnalyzer in the topology to display more information in a tooltip.

**Fabric Settings**

Status: Supervisor Member

Cluster Name: Fabric-22596

Session Port: 6443

Secure Connection: ☒

**Apply**

**Fabric Members**

**supervisor**  
eFAZ-50

Hostname: FAZ-VM22090051  
Role: Member  
Status: In Sync  
IP: 10.8.74.214  
Serial No.: FAZ-VM22090051  
UID: 2611456110  
Version: v7.4.0-build2165  
230222 (Interim)  
Platform Name: FortiAnalyzer-VM64  
Platform Type: FAZVM64  
Auth State: Pending  
Last Ping Change: 2023-03-17 02:35:21  
Last Ping Time: 2023-03-17 02:35:20  
Disk Usage Free: 470.38GB  
Disk Usage Total: 491.15GB  
Ip: 10.8.74.214

**member**  
FAZ-VM22090051

IP: 10.8.74.214

**member**  
FAZ-VM23003360

IP: 10.3.120.54

You can also see the topology in the supervisor's **Log View**. Hover over a FortiAnalyzer in the *FortiAnalyzer Host Name* column to view the topology in a tooltip.

**eFAZ-50** Supervisor

Dashboard | Device Manager | **Log View** | Fabric | FortiGate | FortiAnalyzer | Fabric View | Incidents & Events | Management Extensions | System Settings

Traffic | Security | Event

eFAZ-54 | Last 5 Minutes | 16:46:38 To 16:51:37

Add Filter

#	FortiAnaly...	ADOM	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application
1	eFAZ-54	Name: eFAZ-54		DETK180126	close	10.2.120.5		196.45.45.45	tcp/853	tcp/853
2	eFAZ-54	Status: Online		1FTK190016	deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
3	eFAZ-54	Role: Member		DETK180126	timeout	10.3.120.20		10.2.174.135	tcp/514	tcp/514
4	eFAZ-54	IP: 10.3.120.54		1FTK190016	deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
5	eFAZ-54	Topology: FAZ-VM22090051		1FTK190016	deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
6	eFAZ-54	FAZ-VM23003360		DETK180126	deny	fe80::ae1f:6bff:fece:d2e		ff02::1:2	DHCP6	DHCP6
7	eFAZ-54	FAZ-VM22090040		DETK180126	deny	fe80::ae1f:6bff:fece:d2e		ff02::1:2	DHCP6	DHCP6
8	eFAZ-54	fortinet	16:51:09	FGT80ETK180126	deny	fe80::ec4:7aff:fe7f:482		ff02::1:2	DHCP6	DHCP6

### FortiAnalyzer Fabric member:


To view the topology on a member, go to **System Settings > Fabric Management > Fabric Settings**. In the *Fabric Members* section, the topology displays only the connection to the supervisor. It does not display the other members in the FortiAnalyzer Fabric.


Fabric Settings

Status	<input checked="" type="checkbox"/>
Role	Supervisor Member
Cluster Name	Fabric-22596
IP	10.2.120.50
Session Port	6443
Secure Connection	<input checked="" type="checkbox"/>
Authorization	Accepted

Apply

Fabric Members

 supervisor  
FAZ-VM2M22008021  
IP: 10.3.120.50

 member  
eFAZ-54  
IP: 10.3.120.54

## Fabric of FAZ: member authorization with supervisor



This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- [Configuring the FortiAnalyzer Fabric](#)

The FortiAnalyzer Fabric authentication process has been enhanced by implementing the following:

- Members can join the FortiAnalyzer Fabric by entering the cluster name and IP of the supervisor. No static password is required.
- The supervisor can authorize and reject members from joining the FortiAnalyzer Fabric.
- A `trusted-list` can be configured on the FortiAnalyzer Fabric supervisor to automatically authorize members if they match the configured serial number.
- A `trusted-list` can be configured on FortiAnalyzer Fabric members, so that they will join the FortiAnalyzer Fabric only if the supervisor matches the configured serial number.

### FortiAnalyzer Fabric supervisor:

When configuring a FortiAnalyzer Fabric supervisor in *System Settings > Fabric Management*, there is no password configuration in the *Fabric Settings*.

Fabric Settings

Status	<input checked="" type="checkbox"/>
Role	Supervisor Member
Cluster Name	Fabric-22596
Session Port	6443
Secure Connection	<input checked="" type="checkbox"/>

Apply

When members join the FortiAnalyzer Fabric, they will display in the topology for the supervisor. From this topology in the supervisor, you can authorize or reject the members.

Fabric Settings

Status ☒

Role **Supervisor** Member

Cluster Name Fabric-22596

Session Port 6443

Secure Connection ☒

Apply

Fabric Members

```
graph TD; S[supervisor eFAZ-50 IP: 10.3.120.50] --- M1[member FAZ-VMTM22090051 IP: 10.8.74.214]; S --- M2[member FAZ-VMTM23003360 IP: 10.3.120.54]; S --- M3[member FAZ-VMTM22090040 IP: 10.8.74.99];
```

The topology diagram shows a central supervisor node labeled 'supervisor eFAZ-50' with IP '10.3.120.50'. It is connected to three member nodes: 'member FAZ-VMTM22090051' (IP: 10.8.74.214), 'member FAZ-VMTM23003360' (IP: 10.3.120.54), and 'member FAZ-VMTM22090040' (IP: 10.8.74.99). Each member node has an 'Authorize' button (green checkmark) and a 'Reject' button (red X).

If authorized, the member will join the FortiAnalyzer Fabric and it will remain visible in the topology.

Fabric Settings

Status ☒

Role **Supervisor** Member

Cluster Name Fabric-22596

Session Port 6443

Secure Connection ☒

Confirm Operation

Are you sure you want to authorize selected device?

OK Cancel

Fabric Members

```
graph TD; S[supervisor eFAZ-50 IP: 10.3.120.50] --- M1[member FAZ-VMTM22090051 IP: 10.8.74.214]; S --- M2[member FAZ-VMTM23003360 IP: 10.3.120.54]; S --- M3[member FAZ-VMTM22090040 IP: 10.8.74.99];
```

The topology diagram is identical to the one above, showing the supervisor node connected to three member nodes. The 'Confirm Operation' dialog box is overlaid on the interface, asking for confirmation to authorize the selected device.

Fabric Settings

Status

☒

Role

Supervisor

Member

Cluster Name

Fabric-22596

Session Port

6443

Secure Connection

☒

Apply

Fabric Members

supervisor

eFAZ-50

IP: 10.3.120.50

member

FAZ-VM2M22090051

IP: 10.8.74.214

member

FAZ-VM2M23003360

IP: 10.3.120.54

member

FAZ-VM2M22090040

IP: 10.8.74.99

If rejected, the member will be removed from topology and it will be blocked from attempting to re-join the FortiAnalyzer Fabric for 10 minutes.

Fabric Settings

Status

☒

Role

Supervisor

Member

Cluster Name

Fabric-22596

Session Port

6443

Secure Connection

☒

Confirm Operation

Are you sure you want to reject selected device?

OK

Cancel

Fabric Members

eFAZ-50

IP: 10.3.120.50

member

FAZ-VM2M21007826

IP: 10.3.120.204

Authorize

Reject

member

FAZ-VM2M22090051

IP: 10.8.74.214

member

FAZ-VM2M23003360

IP: 10.3.120.54

Fabric Settings

Status

☒

Role

Supervisor

Member

Cluster Name

Fabric-22596

Session Port

6443

Secure Connection

☒

Apply

Fabric Members

supervisor

eFAZ-50

IP: 10.3.120.50

member

FAZ-VM2M22090051

IP: 10.8.74.214

member

FAZ-VM2M23003360

IP: 10.3.120.54

member

FAZ-VM2M22090040

IP: 10.8.74.99

### FortiAnalyzer Fabric members:

When joining a FortiAnalyzer Fabric as a member, go to *System Settings > Fabric Management*. You do not need to enter a password. Instead, enter the cluster name and IP of the supervisor.

Fabric Settings

Status

☒

Role

Supervisor

Member

Cluster Name

Fabric-22596

IP

10.2.120.50

Session Port

6443

Secure Connection

☒

Apply

After configuring the FortiAnalyzer as a member, the *Authorization* field will display *Pending*.

Fabric Settings

Status

☒

Role

Supervisor

Member

Cluster Name

Fabric-22596

IP

172.18.78.50

Session Port

Secure Connection

☒

Authorization

Pending

Apply


Once the member is authorized by the supervisor, the *Authorization* field will change to *Accepted*. The topology will display this member and the supervisor, but it will not display other members in the FortiAnalyzer Fabric.

Fabric Settings

Status	<input checked="" type="checkbox"/>
Role	Supervisor Member
Cluster Name	Fabric-22596
IP	172.18.78.50
Session Port	
Secure Connection	<input checked="" type="checkbox"/>
Authorization	Accepted

Apply


Fabric Members



SUPERVISOR

FAZ-VMTM22008021

IP: 10.3.120.50



MEMBER

FAZ-VMTM22090051

IP: Local

If the member is rejected by the supervisor, the *Authorization* field will change to *Rejected*. The member must wait 10 minutes before sending another request to join the FortiAnalyzer Fabric. To try again, click apply after the block-out time is complete.


Fabric Settings

Status	<input checked="" type="checkbox"/>
Role	Supervisor Member
Cluster Name	Fabric-22596
IP	10.2.120.50
Session Port	6443
Secure Connection	<input checked="" type="checkbox"/>
Authorization	Rejected

Apply

To leave a FortiAnalyzer Fabric, go to *System Settings > Fabric Management > Fabric Settings* in the member and set the *Status* to disabled. A message will display to confirm the action.

Fabric Settings

Status 

Leaving FortiAnalyzer Fabric?

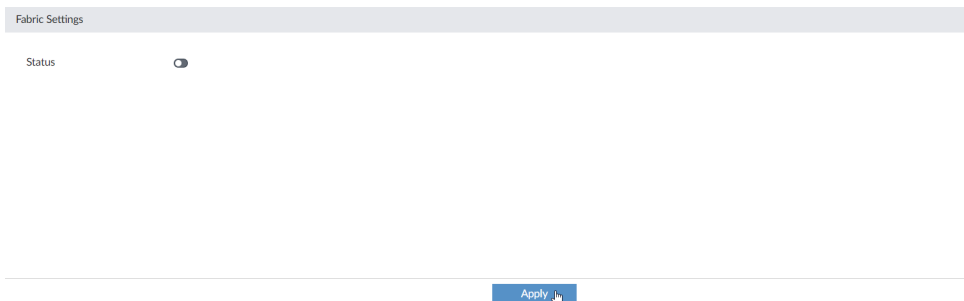
If you proceed, you will be leaving the FortiAnalyzer Fabric. Are you sure you want to leave?

Confirm

Cancel

After confirming the message, click *Apply* to save the configuration.





If needed, the member can re-join the FortiAnalyzer Fabric, but it will need to be authorized by the supervisor again.

### Trusted-list for a FortiAnalyzer Fabric:

The `trusted-list` configuration is completed on the CLI for both the supervisor and the members.

In the supervisor's CLI, you can add members' serial numbers to a `trusted-list`. This supports wildcard; for example, `FAZ-VMTM120033*`. Once a member's serial number is added to the `trusted-list`, that FortiAnalyzer can automatically join the FortiAnalyzer Fabric as a member without the supervisor's authorization.

To add a member to the `trusted-list`, enter the following command in the supervisor's CLI:

```
config system soc-fabric
config trusted-list
edit 1
set serial <member's serial number, which can include wildcards (*)>
end
end
```

In the member's CLI, you can configure a `trusted-list` with the supervisor's serial number to verify the legitimacy of the supervisor. This prevents data leakage to a falsified supervisor. Members will only join the FortiAnalyzer Fabric when the supervisor's serial number matches the members `trusted-list`.

To configure a `trusted-list` on a member, enter the following command in the member's CLI:

```
config system soc-fabric
config trusted-list
edit 1
set serial <Supervisor's serial number>
end
end
```

For members without a `trusted-list` configured, they will treat all supervisors as legitimate.

## Fabric of FAZ global FortiView support

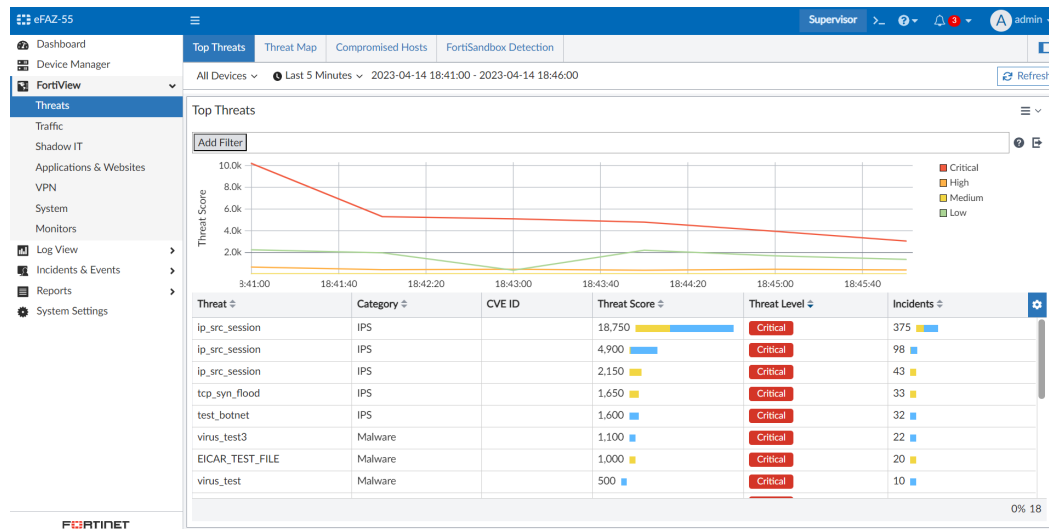


This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

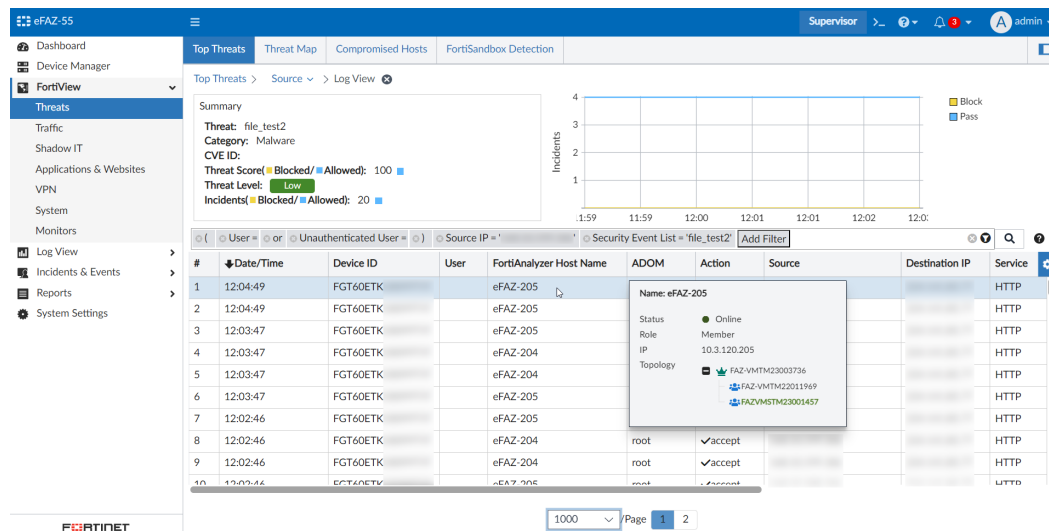
- [FortiView](#)

The FortiAnalyzer supervisor allows you to see FortiView analytics across the entire FortiAnalyzer Fabric. For more granular analysis, you can filter by the FortiAnalyzer members or ADOMs.

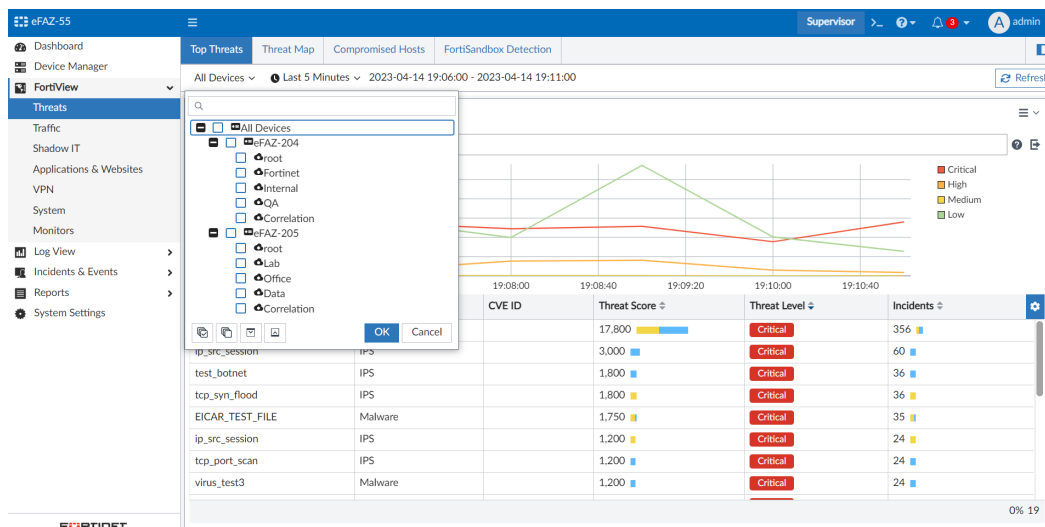
In the FortiAnalyzer Fabric supervisor, go to the *FortiView* panes. The information in these panes are generated from all members in the Fabric cluster. See the below example of *FortiView > Threats > Top Threats*.



Double-click an entry to drill down to a *Log View* of the information. In this view, you can determine the member using the *FortiAnalyzer Host Name* column.



You can also filter the *FortiView* panes by the Fabric members or ADOMs in the device list.



## Fabric of FAZ: Central report support and creating Fabric groups



This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- [Reports](#)
- [Fabric Groups](#)

Reports can now be executed from the Fabric supervisor that fetches and aggregates data from multiple FortiAnalyzer Fabric members. Reports are centrally visible on the supervisor.

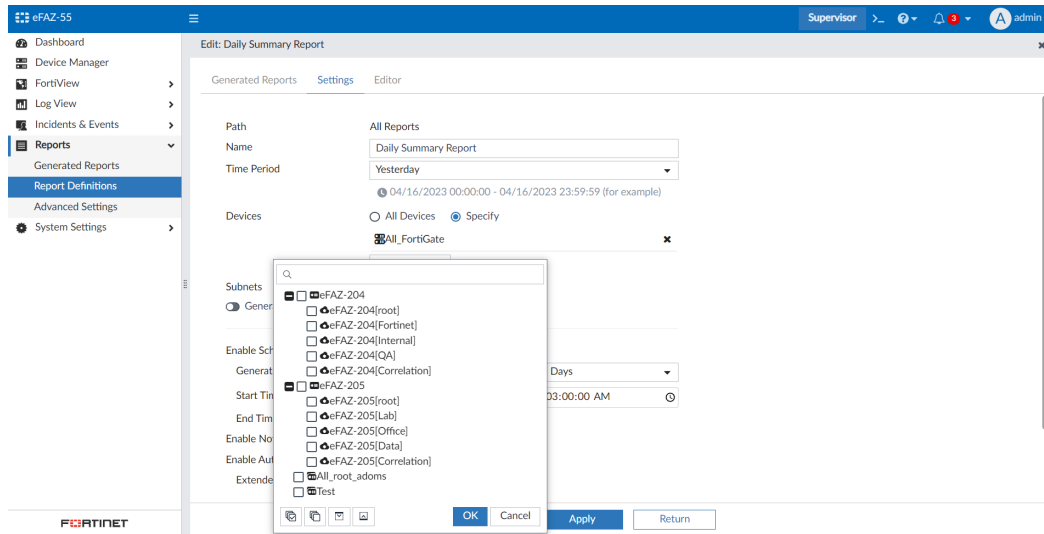
Additionally, FortiAnalyzer Fabric members or ADOMs can be grouped in a Fabric Group, which can be used in the *Log View*, *FortiView* and *Reports* device filter.

### Reports:

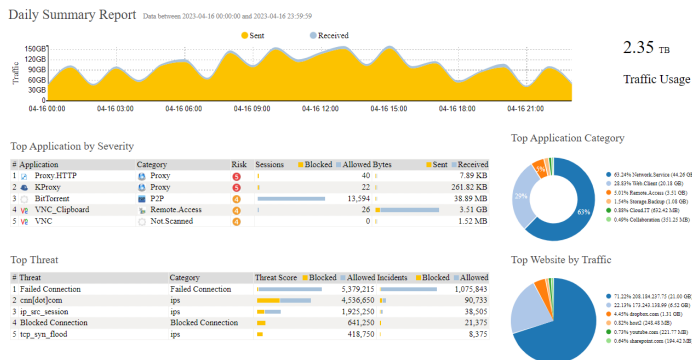
The *Reports* panes are available in the FortiAnalyzer Fabric supervisor.

Title	Language	Cache Status	Time Period	Devices	Schedule	Config Recommendation	Out
<input type="checkbox"/> Application Reports							
<input type="checkbox"/> Asset and User Reports							
<input type="checkbox"/> Compliance Reports							
<input type="checkbox"/> Fabric Reports							
<input type="checkbox"/> FortiCache Reports							
<input type="checkbox"/> FortiClient Reports							
<input type="checkbox"/> FortiDDoS Reports							
<input type="checkbox"/> FortiDeceptor Reports							
<input type="checkbox"/> FortiFirewall Reports							
<input type="checkbox"/> FortiGate Reports							
<input type="checkbox"/> FortiMail Reports							
<input type="checkbox"/> FortiNAC Reports							
<input type="checkbox"/> FortiNDR Reports							
<input type="checkbox"/> FortiProxy Reports							
<input type="checkbox"/> FortiSandbox Reports							
<input type="checkbox"/> FortiWeb Reports							
<input type="checkbox"/> Network Reports							
<input type="checkbox"/> Outbreak Alert Reports							

In the supervisor, you can edit a report to specify which devices (Fabric members, ADOMs, and Fabric Groups) to include when running the report.



The reports' formats, charts, and tables are the same as a regular FortiAnalyzer's, but they include aggregated results from all the selected members.



### To create a Fabric Group in a FortiAnalyzer Fabric:

1. In the FortiAnalyzer Fabric supervisor, go to *System Settings > Fabric Management > Fabric Groups*.

<div><div><div><div><div></div><div>Create New</div></div><div><div><div></div><div>Edit</div></div><div><div><div></div><div>Delete</div></div></div></div></div><div>Search...</div></div></div>						
Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/...	Device Storage	Description
All_root_adoms 2						
<div><div><div></div><div>eFAZ-204</div></div><div>root</div></div>	10.3.120.204	FortiAnalyzer-VM64				
<div><div><div></div><div>eFAZ-205</div></div><div>root</div></div>	10.3.120.205	FortiAnalyzer-VM64				

2. Click *Create New*.
3. In the *Group Name* field, enter a name for the Fabric Group.
4. In the *Add Member* section, select the FortiAnalyzer Fabric members to include.

To add only specific ADOMs from the member, expand the member in the list and select the ADOMs to include.

Create Fabric Group

Group Name: Test

Description:

Add Member

Search...

- ☐ eFAZ-204
- ☐ eFAZ-205
- ☐ Correlation
- ☒ Data
- ☐ FortiAnalyzer
- ☐ FortiAuthenticator
- ☐ FortiCache
- ☐ FortiCarrier

2 entries selected

OK Cancel

##### 5. Click OK.

The Fabric Group can now be edited or deleted from the table.

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/...	Device Storage	Description
All_root_adoms						
eFAZ-204	10.3.120.204	FortiAnalyzer-VM64				
root						
eFAZ-205	10.3.120.205	FortiAnalyzer-VM64				
root						
Test						
eFAZ-204	10.3.120.204	FortiAnalyzer-VM64				
QA						
FGT61F-V64	10.2.60.43	FortiGate-61F	Real Time	N/A	0%	
FGT101E-2	10.2.60.41	FortiGate-101E	Real Time	N/A	0.2%	
eFAZ-205	10.3.120.205	FortiAnalyzer-VM64				
root						
eFGT-HA_FGVULV	10.3.120.201	FortiGate-VM64	Real Time	N/A	0%	
SYSLOG-0A0378...	10.3.120.232	Syslog-Device	Real Time	N/A	0%	
FG100D3G12800...	10.2.0.150	FortiGate-100D	Real Time	N/A	0%	
FortiGate-1500D	10.2.0.250	FortiGate-1500D	Real Time	N/A	0%	
FG3K6ETB19900...	10.2.0.250	FortiGate-3600E	Real Time	N/A	0%	
eFGT-201	10.3.120.201	FortiGate-VM64	Real Time	N/A	0%	

The Fabric Group is also visible in *Device Manager*.

Fortinet Supervisor Dashboard

Search...

Dashboard

Device Manager

FortiView

Log View

Incidents & Events

Reports

System Settings

Fabric M...

ADOMs

Device T...

Status

Critical ...

125

10

125

125

6,710

Name	IP Address	Platform	Logs	Serial Number	Average Log Rate(Logs/...	Device Storage	Description
eFAZ-204	10.3.120.204	FortiAnalyzer-VM64		FAZ-VM64			
root							
eFGT-HA_FGVULV	10.3.120.201	FortiGate-VM64	Real Time	FGVULV	N/A	0%	
root			Real Time	vdsm	N/A	0%	
PWF61E-V64	10.2.0.250	FortiWiFi-61E	Real Time	PWF61ETK	5	7.39%	
root			Real Time	vdsm	5	7.39%	
FW-93-FCT	192.168.125.1	FortiGate-VM64	Real Time	FGVM04TM	N/A	0%	
root			Real Time	vdsm	N/A	0%	
FG100D3G12800081	10.2.0.150	FortiGate-100D	Real Time	FG100D3G	N/A	0%	
root			Real Time	vdsm	N/A	0%	
FortiGate-1500D	10.2.0.250	FortiGate-1500D	Real Time	FG1KSD3I	N/A	0%	
root			Real Time	vdsm	N/A	0%	
FG3K6ETB19900075	10.2.0.250	FortiGate-3600E	Real Time	FG3K6ETB	N/A	0%	
root			Real Time	vdsm	N/A	0%	
FCTEM50000114212	10.3.120.247	FortiClient-EM5	Real Time	FCTEM50000	N/A	0.04%	
default			Real Time	vdsm	N/A	0.04%	
eFGT-80E	10.3.120.254	FortiGate-80E	Real Time	FGT80ETK	3	2.89%	
root			Real Time	vdsm	3	2.89%	

0% 296

It can be selected in the device filter for *FortiView*, *Log View*, and *Reports*. See an example in *Log View* below.

User	FortiAnalyzer Host Name	ADOM	Action	Source	Destination IP	Service
eFAZ-204	QA	✓accept	192.168.1.119	10.2.60.103	tcp/514	
eFAZ-205	root	✗deny	fe80::2c76:6055:f8a4:bbd1	#02:c	udp/1900	
eFAZ-205	root	✓close	10.3.120.29	96.45.46.46	tcp/853	
eFAZ-205	root	✗deny	fe80::2c76:6055:f8a4:bbd1	#02:c	udp/1900	
eFAZ-205	root	✗deny	fe80::2c76:6055:f8a4:bbd1	#02:c	udp/1900	
eFAZ-205	root	✓close	10.3.120.29	96.45.46.46	tcp/853	
eFAZ-204	QA	✗deny	0.0.0.0	255.255.255.255	DHCP	
rachel	eFAZ-204	QA	✓close	rachel (10.212.137.200)	10.2.90.106	HTTPS
rachel	eFAZ-204	QA	✓accept	192.168.1.101	192.168.2.102	tcp/514
rachel	eFAZ-204	QA	client-rst	rachel (10.212.137.200)	10.2.60.82	HTTPS
eFAZ-205	root	✗deny	fe80::2c76:6055:f8a4:bbd1	#02:c	udp/1900	
eFAZ-205	root	✗deny	fe80::2c76:6055:f8a4:bbd1	#02:c	udp/1900	
eFAZ-204	QA	✗deny	10.2.175.110	10.2.175.255	udp/138	
eFAZ-204	QA	✗deny	0.0.0.0	255.255.255.255	DHCP	
rachel	eFAZ-204	QA	client-rst	rachel (10.212.137.200)	10.2.90.106	HTTPS
eFAZ-204	QA	✗deny	10.2.60.107	255.255.255.255	udp/6666	
eFAZ-204	QA	✗deny	0.0.0.0	255.255.255.255	DHCP	

## Block out contract device from upgrading to next or major or minor release



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [Updating the system firmware.](#)
- [Updating the system firmware](#)

### To view available FortiGuard images:

1. A FortiAnalyzer with a valid contract will display all available FortiGuard images and allow upgrading or downgrading to any version.

- System Settings:

Firmware Management

Current Version

v7.0.3-build1362 230210 (Interim)

Upload Firmware

Add files by drag & drop here or [Add Files](#)

FortiGuard Firmware

7.2.2 (1334)

Backup Configuration

Q

Encryption

✓ 7.2.2 (1334)

7.2.1 (1215)

7.2.0 (1124)

7.0.4 (306)

7.0.3 (254)

7.0.2 (180)

6.4.10 (2549)

6.4.9 (2513)

OK

Cancel

2. A FortiAnalyzer without a valid contract or with an expired contract will only display available patch images and support patch upgrades.

- System Settings:

Firmware Management

Current Version

v7.0.3-build0237 230215 (Interim)

Upload Firmware

Add files by drag & drop here or [Add Files](#)

FortiGuard Firmware

7.0.4 (306)

Backup Configuration

Q

Encryption

✓ 7.0.4 (306)

7.0.3 (254)

7.0.2 (180)

OK


Cancel



- FortiAnalyzer setup wizard:

FortiManager Setup - Upgrade Firmware (3/4)

Upgrade Firmware


 A new firmware version is available

Current Version

v7.0.2-build0180 230209 (Interim)

Latest Version

7.0.4 (306)

 [Release Notes](#)

Backup Configuration

☒

Encryption

☐

Next >

Later

# Cloud Services

This section lists the new features added to FortiAnalyzer for cloud services:

- FortiAnalyzer supports FortiCare Elite Service on page 70

## FortiAnalyzer supports FortiCare Elite Service

FortiAnalyzer and FortiAnalyzer Cloud now supports FortiCare Elite Service.

To use this service, cloud management must be enabled on the FortiAnalyzer and the FortiGate Cloud portal.

The screenshot displays the FortiAnalyzer GUI. The top section shows 'License Information' with details for VM License (Valid 10K-UG, Registered, Cloud Management), FortiCloud (Indicators of Compromise, Not Licensed), FortiGuard (FortiAnalyzer Outbreak D..., No License), Security Operations (Security Automation, Not Licensed; Industrial Security Service, Not Licensed; Security Rating Update, Not Licensed), and Logging (Devices/VDOMs: 3 / 10,000 (0.0%)).

The bottom section shows the 'FortiGate Cloud' portal with a table of assets:

Assets	SN	Name	Firmware	Status	SD-WAN	Management Connectivity	Subsc
<input type="checkbox"/>	FAZ-VM1TM22090591	FAZVM64	7.4.0	CPU 8% Memory 22%			
<input type="checkbox"/>	FGVM04TM22090093						
<input type="checkbox"/>	FGVM04TM22090094						
<input type="checkbox"/>	FGVM04TM22090150	fgt06-fnt02	7.0.5				

Log forwarding configuration to the Elite Service can be viewed in the FortiAnalyzer GUI. This log forwarding configuration cannot be edited or deleted.

The screenshot displays the 'Log Forwarding' configuration page in the FortiAnalyzer GUI. It shows a table with log forwarding settings:

Server Name	Forward Logs to	Device Filters	Forward Logs Frequency	Output Profile
elite	Elite Service(172.16.94.93)	[root]FGVMSLTM22002986, [root]FGVMSLTM22003023, [root]	Real-time	N/A

The log forward configuration to Elite Service is also visible in the FortiAnalyzer CLI. For example:

```
config system log-forward
edit 40000
set mode forwarding
set fwd-max-delay realtime
```

```
set server-name "elite"
set server-addr "172.16.94.93"
set fwd-server-type elite-service
set fwd-reliable enable
set fwd-compression enable
set fwd-archives disable
set proxy-service disable
  config device-filter
    edit 1
      set action include-like
      set device "*"
    next
  end
set log-filter-status enable
  config log-filter
    edit 1
      set field level
      set oper >=
      set value "critical"
    next
    edit 2
      set field logid
      set value "0110052000"
    next
  end
set signature 1449934396
next
```

You can disable the Elite Service in the FortiAnalyzer CLI, if needed. It can also be re-enabled using the same command. In the FortiAnalyzer CLI, enter:

```
config system central-management
  set elite-service {enable | disable}
end
```

If `elite-service` is disabled, the log forwarding to Elite Service will automatically be removed. FGC will push the configuration back if the `elite-service` is later set to `enable`.

```
FAZVM64 # config system central-management
(central-management)# get
type : cloud-management
elite-service : enable
```

Logs that meet the filter within the log forward configuration will be forwarded to Elite log server. See a sample log in the FortiAnalyzer GUI below:

#	A	Date/Time	Level	Device ID	Log Description	Security Rating Score
1		10:30:30	notice	FGVMSLTm22003023	Security Rating summary	274.5
2		10:30:30	notice	FGVMSLTm22003023	Security Rating summary	85.0
3		10:30:30	notice	FGVMSLTm22003023	Security Rating summary	240.0
4		10:20:30	notice	FGVMSLTm22002986	Security Rating summary	274.5
5		10:20:30	notice	FGVMSLTm22002986	Security Rating summary	85.0
6		10:20:30	notice	FGVMSLTm22002986	Security Rating summary	240.0
7		06:20:28	notice	FGVMSLTm22003023	Security Rating summary	274.5
8		06:20:28	notice	FGVMSLTm22003023	Security Rating summary	85.0
9		06:20:28	notice	FGVMSLTm22003023	Security Rating summary	240.0
10		06:10:28	notice	FGVMSLTm22002986	Security Rating summary	274.5
11		06:10:28	notice	FGVMSLTm22002986	Security Rating summary	85.0
12		06:10:28	notice	FGVMSLTm22002986	Security Rating summary	240.0
13		02:10:31	notice	FGVMSLTm22003023	Security Rating summary	274.5
14		02:10:26	notice	FGVMSLTm22003023	Security Rating summary	85.0
15		02:10:26	notice	FGVMSLTm22003023	Security Rating summary	240.0
16		02:00:32	notice	FGVMSLTm22002986	Security Rating summary	274.5

### Sample logs from Elite log server:

```
2023-04-14 13:50:42,136 DEBUG Processing /dev/shm/fams/log_upload/proc/FAZ-
VMTM22090591.1264692.nrt.e.1681505055.562204.34406
2023-04-14 13:50:42,137 DEBUG Create new raw log file: elog_20230414_135042 for (*****,
elog)
2023-04-14 13:50:47,083 DEBUG ---sending elite kafka msg---,
elitelogserver.remoteaccessmgr.faz.fsbp, {"action":"downloadFsbpFile","data":
{"fazSn":"FAZ-
VMTM22090591","fgtSn":"FGVMSLTm22002986","auditId":"****","accountId":"****","auditTime"
:1681490426}}}
```

Note that this log forward configuration does NOT impact other types of log forwarding.

The Elite log server can call API to get the Fortinet Security Best Practices (FSBP) reports.

API:

```
{
  "apiver": 3,
  "url": "/fazsys/audittrpt/fgt-orig-rpt",
  "data": {
    "devid": "FGVMSLTm22002986",
    "auditID": "1681505424727"
  }
}
```

```
}  
}
```

The reports are updated in FortiAnalyzer:

```
bash# cd /drive0/private/restapi/audit_rpt/  
bash# ls  
FGVMSLTM22002986          FGVMSLTM22002986_PostureReport    FGVMSLTM22003023_OptimizationReport  
FGVMSLTM22002986_CoverageReport  FGVMSLTM22003023          FGVMSLTM22003023_PostureReport  
FGVMSLTM22002986_OptimizationReport  FGVMSLTM22003023_CoverageReport  
bash#
```



This log forward config does not impact other types of log forward in FortiAnalyzer.

---

# Operational Technology

This section lists the new features added to FortiAnalyzer for Operational Technology:

- [Operational Technology \(OT\) Security Service on page 74](#)
- [OT Purdue Model in a consolidated Asset & Identity Center Dashboard on page 76](#)
- [OT Security Risk Report on page 79](#)

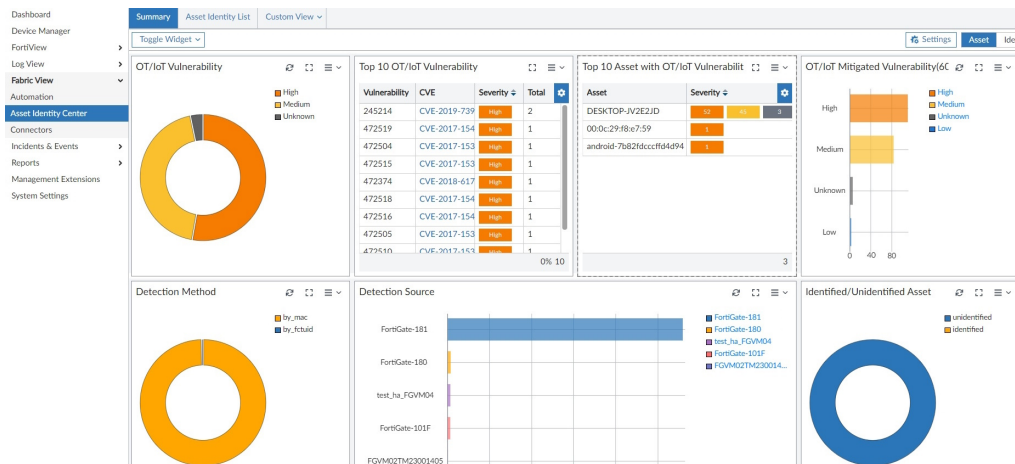
## Operational Technology (OT) Security Service

Upon purchasing the OT Security Service Entitlement, the *Asset Identity Center* in FortiAnalyzer will include valuable information regarding the detected OT/IoT vulnerabilities. This includes information such as:

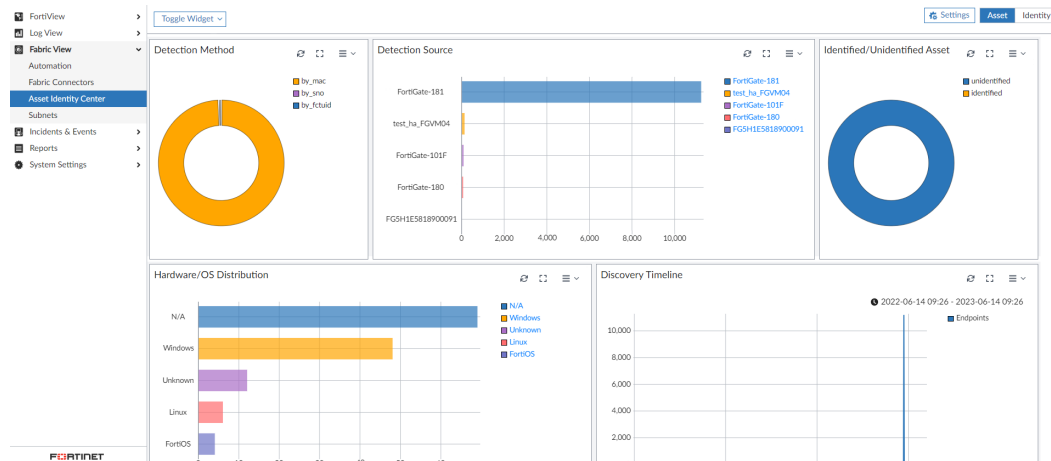
- A breakdown of OT/IoT vulnerabilities with corresponding severity
- Top 10 OT/IoT vulnerabilities by number of occurrences
- Top 10 assets with OT/IoT vulnerabilities
- Details of the vulnerabilities per endpoints

With this service, you can access the following features:

- Go to *Asset Identity Center > Summary* for OT/IoT Vulnerability widgets.



If you do not have a license for the service, the widgets will not be visible.



- Go to **Asset Identity Center > Asset Identity List > Asset List** to view **OT/IoT Vulnerabilities** in the table.

Dashboard	Summary	Asset Identity List	Custom View
Device Manager	Asset List	OT View	
FortiView	Last 1 Week 2023-04-14 10:24:54 - 2023-04-21 10:24:54		
Log View	Custom View Reload More		
Fabric View	Add Filter Asset Identity		
Automation	Endpoint Name	Tags	User MAC Address OT/IoT Vulnerabilities IP Address FortiC
Asset Identity Center	Win-10-1		
Connectors	192.168.174.206		00:0c:29:22:d4:60 192.168.174.25 656F60
Incidents & Events	android-7b82fdcc		00:0c:29:f8:e7:59 192.168.174.206
Reports			88:10:36:23:25:67 192.168.1.2
Management Extensions	FCTEMS0000103259		
System Settings	FCTEMS0000105121		
	FCTEMS2644034189		
	FCTEMS4086893656		
	FCTEMS8821006601		
	FortiGate-101F		
	Stone-FortiGate-80E-POE		
	FGT61F-1		
	FGT91E-1		
	FGVM02TM22010033		
	FortiGate-180		
	FortiGate-181		
	FGVM02TM23001405		
	FGVM02TM23001405		

- Click the numbers in the **OT/IoT Vulnerabilities** column to display the vulnerabilities in more detail, including **Type**, **Severity**, **Reference**, and **Description**.

Dashboard	Summary	Asset Identity List	Custom View
Device Manager	Asset List	OT View	
FortiView	Last 1 Week 2023-04-14 11:23:17 - 2023-04-21 11:23:17		
Log View	Custom View Reload More		
Fabric View	Add Filter Asset Identity		
Automation	Endpoint Name	Tags	
Asset Identity Center	Win-10-1		
Connectors	192.168.174.206		
Incidents & Events	android-7b82fdccfd4d94		
Reports	FCTEMS0000103259		
Management Extensions	FCTEMS0000105121		
System Settings	FCTEMS2644034189		
	FCTEMS4086893656		
	FCTEMS8821006601		
	FortiGate-101F		
	Stone-FortiGate-80E-POE		
	FGT61F-1		
	FGT91E-1		
	FGVM02TM22010033		
	FortiGate-180		
	FortiGate-181		
	FGVM02TM23001405		
	FGVM02TM23001405		

- Click the CVE reference in the **Reference** column to view the details.

**VULNERABILITIES**

### CVE-2017-15402 Detail

**Description**

Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page\_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

**Severity** CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 9.8 CRITICAL Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/LH:A/H

**QUICK INFO**

**CVE Dictionary Entry:** CVE-2017-15402

**NVD Published Date:** 01/09/2019

**NVD Last Modified:** 01/30/2019

**Source:** Google Inc.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

- In the FortiAnalyzer CLI, you can enter the following command to check the status of the endpoint data link between FortiAnalyzer and FortiGate:  

```
diagnose test application oftpd 20 fgt-stat
```

## OT Purdue Model in a consolidated Asset & Identity Center Dashboard



This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- [OT View](#)

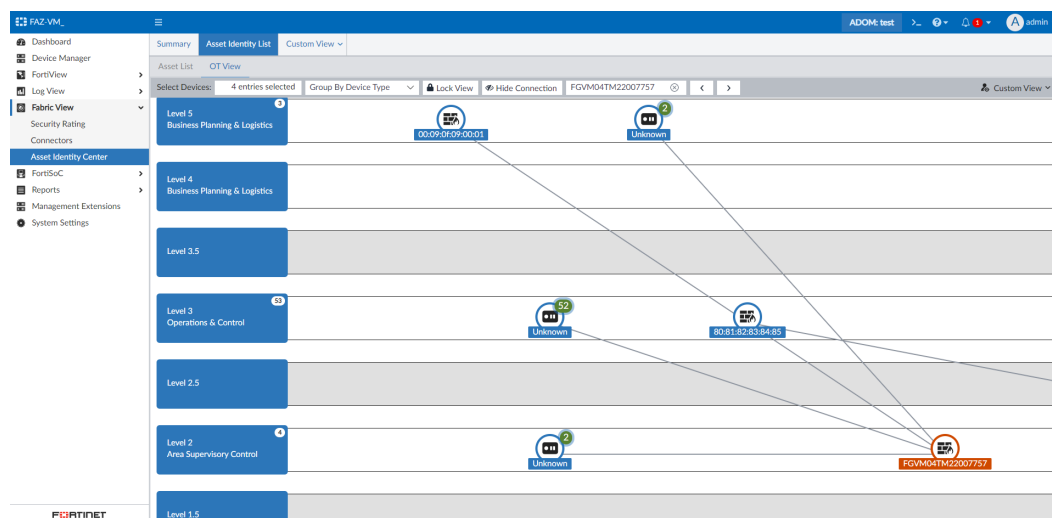
An OT Purdue model has been added to a new and consolidated *Asset & Identity Center*.

This spec introduces a consolidated dashboard for both Assets and Identities: *Fabric View > Asset Identity Center*. In previous versions, Asset and Identity each had a separate dashboard.

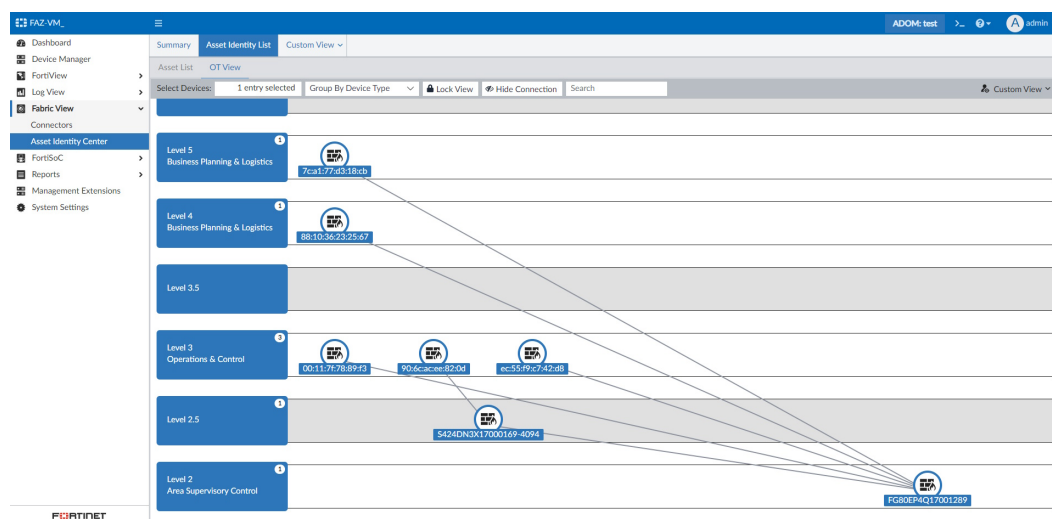
In the new *OT View*, each asset is represented in its corresponding Purdue Layer. All associated endpoints are visible with clear, linear relationships.

To view the new *OT View*, go to *Fabric View > Asset Identity Center > OT View*.

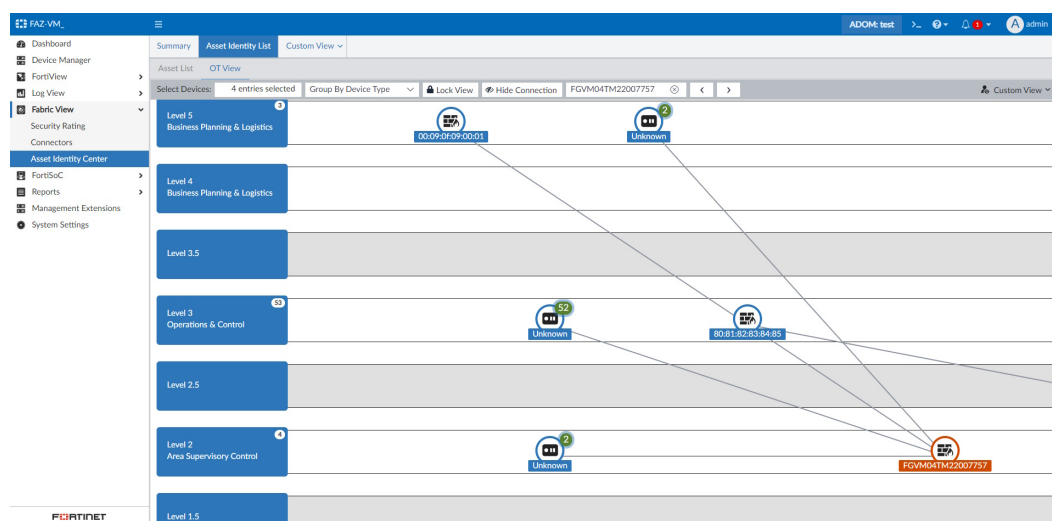




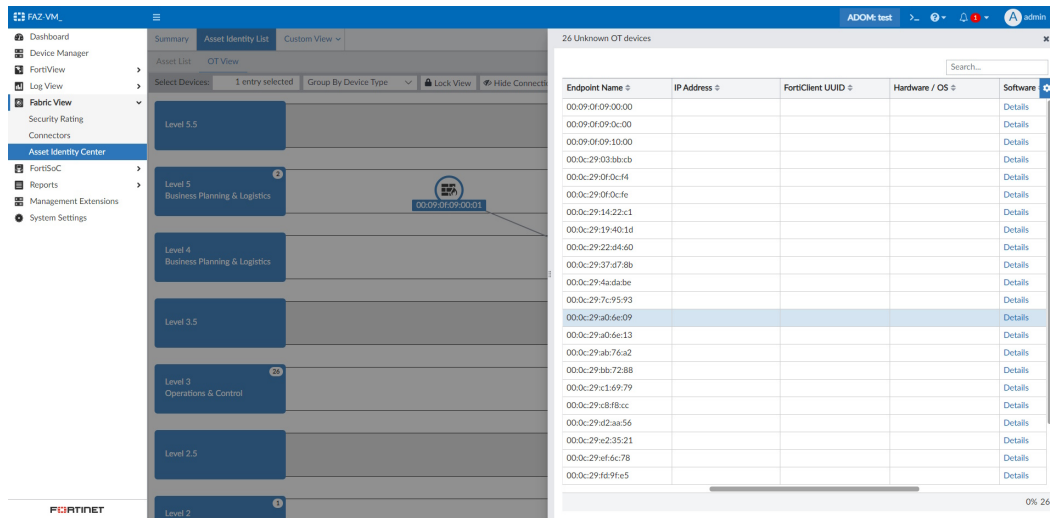
Use the *Select Devices* fields to display all endpoints associated with specified devices.



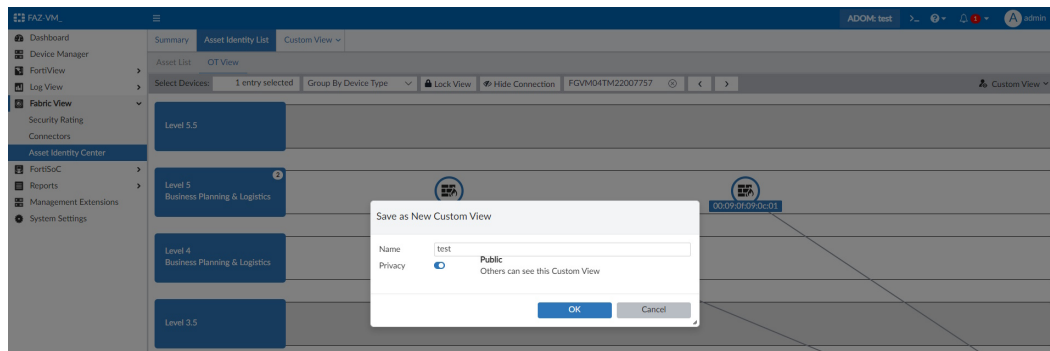
Use the *Search* field to find a specific endpoint, as needed.



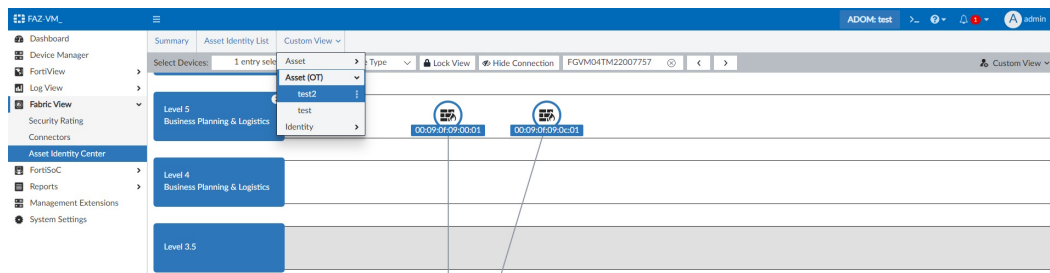
Click an endpoint to review the details of the endpoint or the endpoint's group.



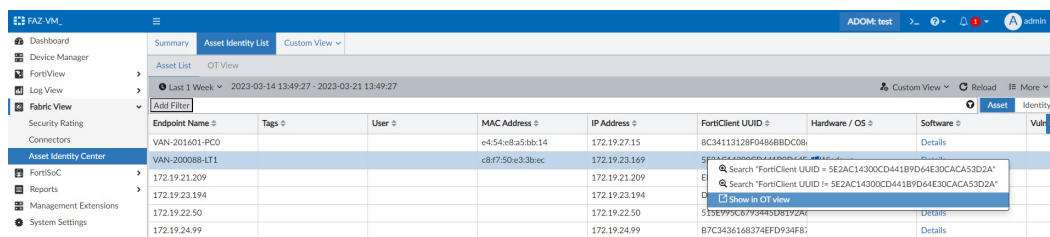
Within the OT View pane, click *Custom View* > *Save As Custom View* to create a custom view.



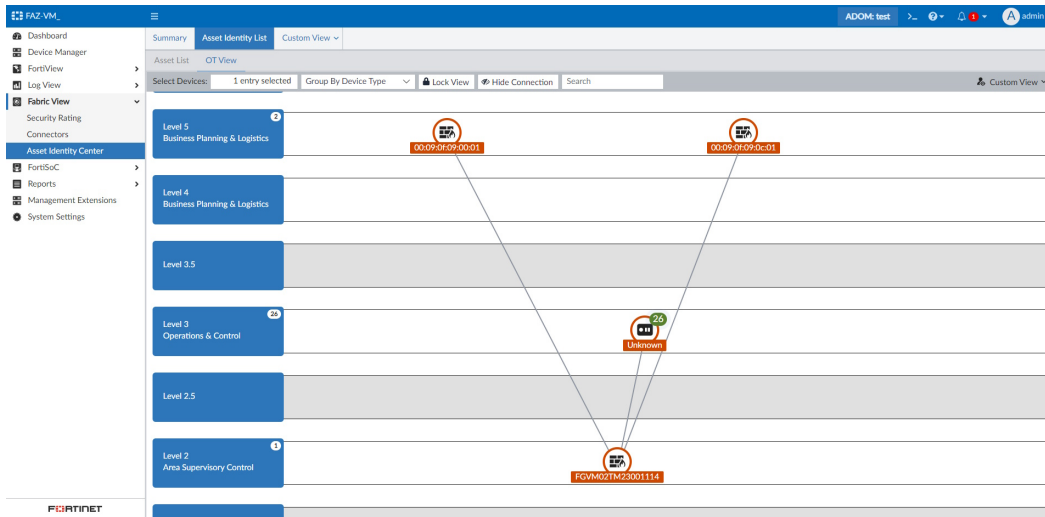
The saved custom views are available in *Fabric View* > *Asset Identity Center* > *Custom View*.



When using *Fabric View* > *Asset Identity Center* > *Asset List*, you can right-click an endpoint and click *Show in OT view* to display it in the OT view instead of the asset list.



After clicking **Show in OT view**, the **Fabric View > Asset Identity Center > OT View** opens to display the selected endpoint.

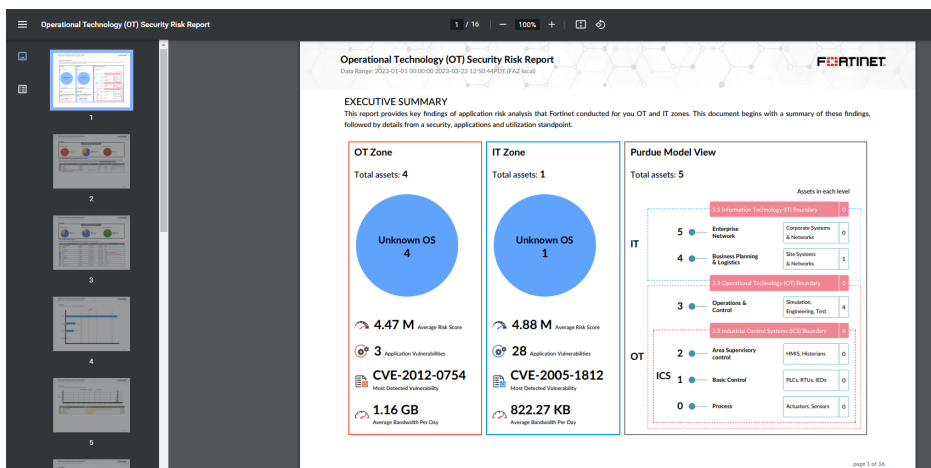


## OT Security Risk Report

An *Operational Technology (OT) Security Risk Report* has been added to provide:

- Application risk analysis for OT and IT zones
- Blind-spot and hidden risks detection
- Purdue Model asset mapping

For example, see a sample of the report in PDF format below:





3. From the *More* dropdown, click *Create Report* to create a report using the template.  
You can also click *Clone* to clone the template and make adjustments.

**To run the Operational Technology (OT) Security Risk Report:**

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *Operational Technology (OT) Security Risk Report*.  
The *Edit: Operational Technology (OT) Security Risk Report* pane opens.
2. Click *Run Report*.  
Once the report is available, click the format to view the report in.

# Index

The following index provides a list of all new features added to FortiAnalyzer 7.4. The index allows you to quickly identify the version where the feature first became available in FortiAnalyzer.

Select a version number to navigate in the index to the new features available for that release:

- [7.4.0 on page 82](#)
- [7.4.1 on page 83](#)

## 7.4.0

### Fabric View

- |            |   |
|------------|---|
| Connectors | • <a href="#">Webhook Connector to Support MS Teams on page 7</a> |
|------------|---|

### Security Operations

- |                    |   |
|--------------------|---|
| Asset and identity | • <a href="#">New charts in the Asset Identity Center on page 9</a> |
| Other enhancements | • <a href="#">FortiSoC GUI reorganization on page 11</a>            |

### Log and Report

- |                    |  |
|--------------------|--|
| Logging            | <ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer supports FortiWeb Cloud attack logs on page 16</a></li><li>• <a href="#">Support parsing and addition of third-party application logs to the SIEM DB on page 17</a></li><li>• <a href="#">Per-ADOM log rate on page 22</a></li></ul>   |
| Log forwarding     | • <a href="#">Fluentd support for public cloud integration on page 30</a>  |
| Reports            | <ul style="list-style-type: none"><li>• <a href="#">Report guidance on page 34</a></li><li>• <a href="#">PCI Security Rating Report on page 36</a></li><li>• <a href="#">Cyber Threats Assessment Report update on page 37</a></li><li>• <a href="#">Threat Report update on page 38</a></li><li>• <a href="#">FSBP Security Rating Report on page 40</a></li><li>• <a href="#">CIS Controls Security Rating report on page 41</a></li><li>• <a href="#">Shadow IT Report on page 42</a></li></ul> |
| Other enhancements | • <a href="#">Time zone settings per ADOMs/Reports on page 46</a>  |

## System

Other enhancements	<ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer GUI enhancements on page 50</a></li><li>• <a href="#">Fabric of FAZ topology chart on page 54</a></li><li>• <a href="#">Fabric of FAZ: member authorization with supervisor on page 56</a></li><li>• <a href="#">Fabric of FAZ global FortiView support on page 61</a></li><li>• <a href="#">Fabric of FAZ: Central report support and creating Fabric groups on page 63</a></li><li>• <a href="#">Block out contract device from upgrading to next or major or minor release on page 66</a></li></ul>
--------------------	--

## Cloud Services

Cloud services	<ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer supports FortiCare Elite Service on page 70</a></li></ul>
----------------	---

## Operational Technology

Operational Technology	<ul style="list-style-type: none"><li>• <a href="#">Operational Technology (OT) Security Service on page 74</a></li><li>• <a href="#">OT Purdue Model in a consolidated Asset &amp; Identity Center Dashboard on page 76</a></li><li>• <a href="#">OT Security Risk Report on page 79</a></li></ul>
------------------------	---

## 7.4.1

## Security Operations

Other enhancements	<ul style="list-style-type: none"><li>• <a href="#">Notifications for new Outbreak Alerts 7.4.1 on page 14</a></li></ul>
--------------------	--

## Log and Report

Logging	<ul style="list-style-type: none"><li>• <a href="#">Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 on page 24</a></li><li>• <a href="#">Logging support for FortiCASB 7.4.1 on page 26</a></li><li>• <a href="#">Logging support for FortiPAM 7.4.1 on page 28</a></li><li>• <a href="#">Logging support for FortiToken Cloud 7.4.1 on page 29</a></li></ul>
Reports	<ul style="list-style-type: none"><li>• <a href="#">FortiADC Report 7.4.1 on page 43</a></li><li>• <a href="#">Default ZTNA Report 7.4.1 on page 45</a></li></ul>



[www.fortinet.com](http://www.fortinet.com)

---

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.